Technical Architecture Framework

May 8, 2000

TIERS Technical Architecture Framework

Purpose

The purpose of this document is to provide an architectural framework for the Texas Integrated Eligibility Redesign System (TIERS) and provide input to the TIERS procurement document. This document along with the Texas Department of Human Services (TDHS) Enterprise Wide Technical Architecture provide a foundation for the effective development and implementation of a system architecture through standards, guidelines and methodologies and defines general requirements to support that architecture. The outcome will be the development of an architecture that is open, scalable, portable, consistent, and modular.

Italicized text (excluding section headings) throughout this document is used to identify specific vendor requirements. For now, these requirements have been captured in the Technical Architecture Framework and may be included in the TIERS procurement document in the future.

Scope

The scope of this document is a framework for standards and requirements for Hardware, System and Application Software, Network Architecture and Telecommunication, Data and Security. For purposes of this document, *Standards* are defined as those de facto and/or formally documented principles accepted by the TDHS concerning the procurement, architecture, implementation and maintenance of information systems. *Requirements* are defined as the specific conditions that must be complied with by internal TDHS staff as well as contract resources.

Sources

The focus of this document is to address all existing standards that apply to the TIERS procurement. The following sources were used as input to creating this document:

- Health and Human Services (HHS) Agencies Information Systems Architecture DRAFT Document
- Health and Human Services Consolidated Network (HHSCN) - 1998 Annual Report
- Texas Department of Human Services Information Systems Architecture

- Texas Department of Human Services Enterprise Wide Technical Architecture
- Information gathering sessions conducted to collect TDHS architectural standards and requirements
- State of Texas Department of Information Resources (DIR) standards publications
- The Federal Government's Federal Information Processing Standard (FIPS) Publications to the extent that they were referenced by State standards
- Generally accepted industry standards

Additions and refinements to standards, methodologies and guidelines will be defined through the consensus of the vendor and TDHS for those areas where standards are not specifically defined.

A. General System Architecture

Overview

The proposed architecture for TIERS must be a modular design based substantially on open systems components that provide flexibility, scalability, and expandability. The modular architecture must be designed to allow incremental change while minimizing the effect on the proposed TIERS hardware and software components. The general system architecture can be broken down into the following specific categories:

- The Technical Architecture provides the framework for interfaces, protocols, standards and products to be used in defining a platform that supports applications across the organization. It is required that any component of the technical architecture can be substituted with another component which provides the same or similar functionality. For example, an existing processing platform can be transitioned from one product to another without affecting the application environment. This framework helps in adopting a structured approach to building the application architecture.
- The Application Architecture provides a framework for the development and use of applications. It enables sharing of common components and data among applications, and provides an integrated set of functions to the user. This framework defines how the applications should be independent of the technical components. Thus, ideally, there should be little effect on

an application if a technical component, such as the TCP/IP stack, is changed or updated.

- The Information Architecture provides a framework for the storing, querying and updating of data. It defines the policy of governing data definition, organization, availability, integrity, privacy, security, resilience, stewardship, distribution, and technologies. The general strategy for this architecture consists of shifting the focus of database design from application support to subject matter representation, developing a single logical view of the data of the enterprise, and partitioning of data into three distinct categories based on its characteristics and uses.

Technical Architecture

Among the various architectures, the n-tiered architecture is a generally accepted model for distributed applications. Using this approach, an application can be split into layers for presentation, business logic and database management. Each layer is independent and has defined interfaces for communication. This architecture facilitates changes in either the presentation, business logic or database management without affecting the other areas. Thus, new presentation services, via Web browser, telephone interfaces, etc., can be plugged-in to the application without affecting the business logic and database functions. Similarly, new database servers can also be added without affecting the presentation and business logic layers. This type of architecture enhances scalability, openness and flexibility.

The TIERS technical architecture must satisfy both the business and technical requirements of the TIERS system. Key components that contribute to this architecture are provided below.

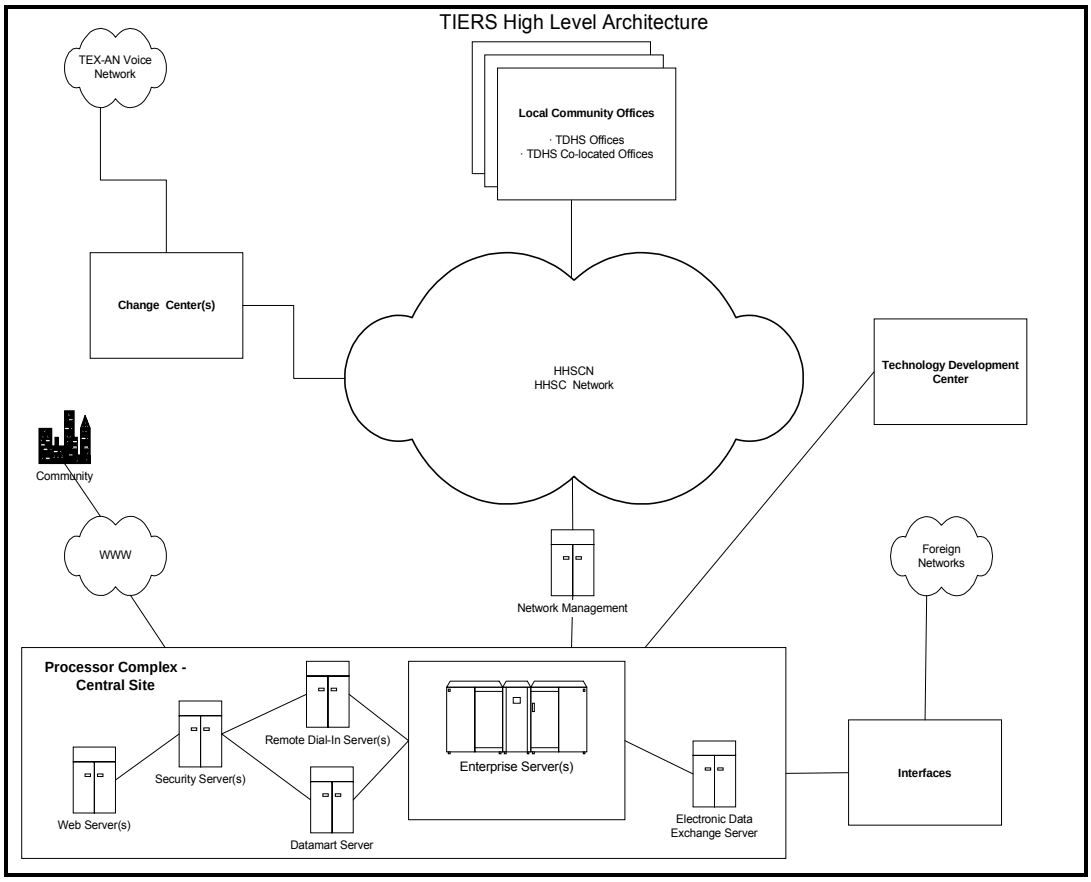


Figure 1 – TIERS High Level Architecture

From a high level view as depicted in Figure 1, the Processor Complex, which provides the centralized portion of application processing, client eligibility determination, rule execution and other required computing functions will interface with the TDHS local offices and Change Centers through the State network infrastructure (HHSCN).

The local offices and change centers will perform eligibility determination activities. It is planned that these local community offices will communicate with the processor complex over the existing State Wide Area Network (WAN) infrastructure. The State requires the utilization of the designated wide area network, HHSCN, in its automated solutions unless a compelling business justification for an alternate approach is demonstrated.

The HHS agencies have developed the HHSCN to reduce costs and facilitate data sharing among the agencies, improve services, leverage existing equipment, technology and support, and increase the negotiation abilities with various network service providers.

The HHSCN has over 900 data circuits, ranging up to T-1 capacity that connect agency local offices. Over 1100 local area networks are connected by the wide area network. There are approximately 20,000 PCs connected to the network (TDHS, PRS, and TDH combined). The majority of these PCs are used to support eligibility determination at TDHS.

Health and Human Services Commission (HHSC) deployed an open systems network architecture, based on router technology and the TCP/IP network protocol. The current backbone configuration provides a high level of redundancy. Most sites have redundant communication abilities to other sites (mainly T-1).

To support business activities of the agency, communication with non-State agencies including Social Security, IRS, Federal Agencies and many other entities, will be required through electronic interfaces. Interfaces with other agencies through foreign networks will be extensive.

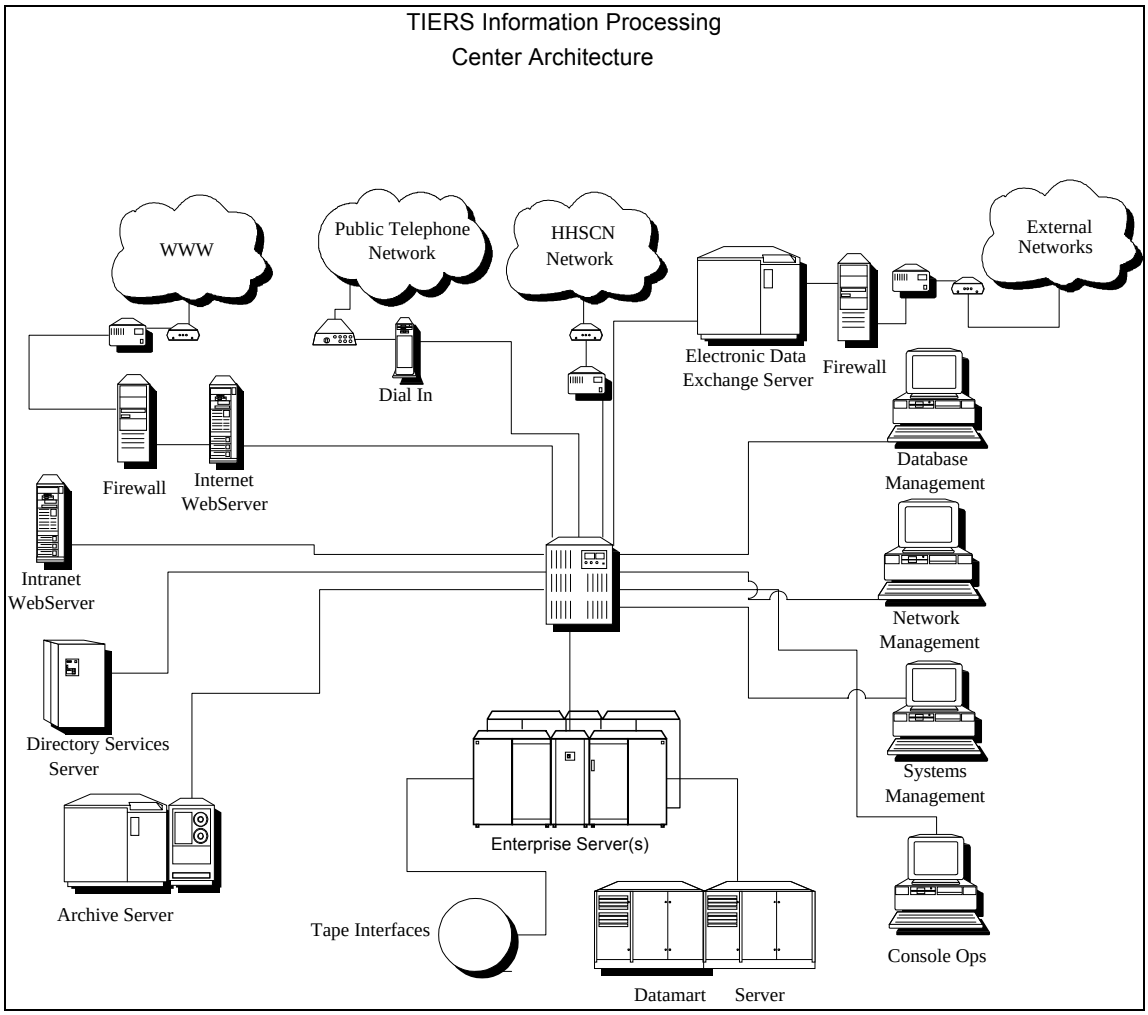


Figure 2 – TIERS Information Processing Center Architecture

Within the Processing Center are areas of functionality represented in Figure 2 as server and workstation icons. The enterprise server(s) are representative of the business rules, and data management functionalities. From these logical servers, a variety of tasks, including systems management, network management, console operations, and database management, will be performed.

The processing of data in aggregate, such as in report generation, data analysis, decision support, and knowledge discovery, are supported on a separate logical, analytical server. This datamart server will be used for mining of production data snapshots. An electronic data exchange server will provide the functionality for interfacing with other agency systems and those systems outside of the State network.

Again, these logical representations are to illustrate functionality only and do not imply that these services must be split out among distinct hardware environments.

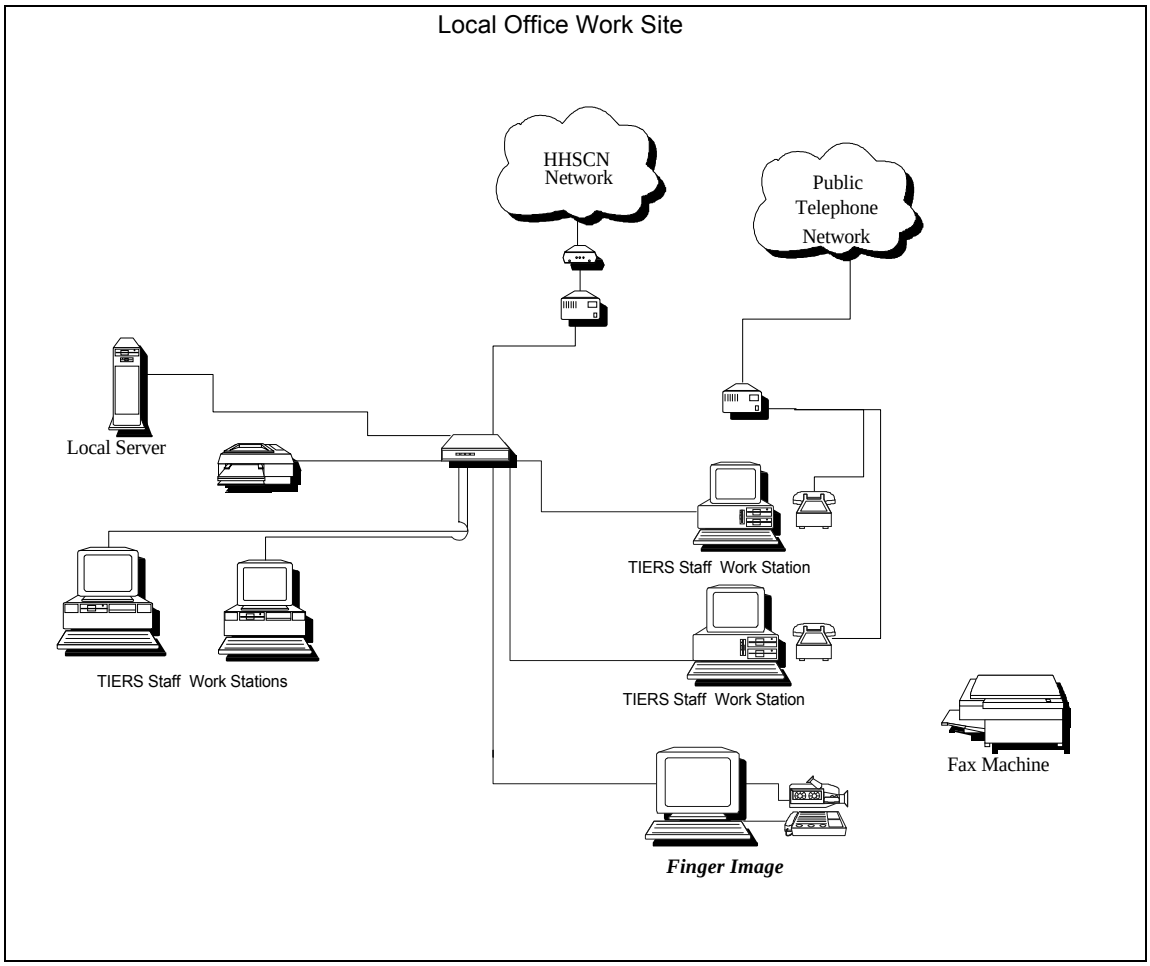


Figure 3 – Local Office Work Site Configuration

The local office work site, depicted in Figure 3, provides State staff with the tools and access needed to interface successfully with the client. As with all of the platforms used by TIERS, other applications may reside on the PCs. Additionally, the local office will be able to send/receive faxes, have local print capability, have access to the Internet and have access to client information to support daily activities.

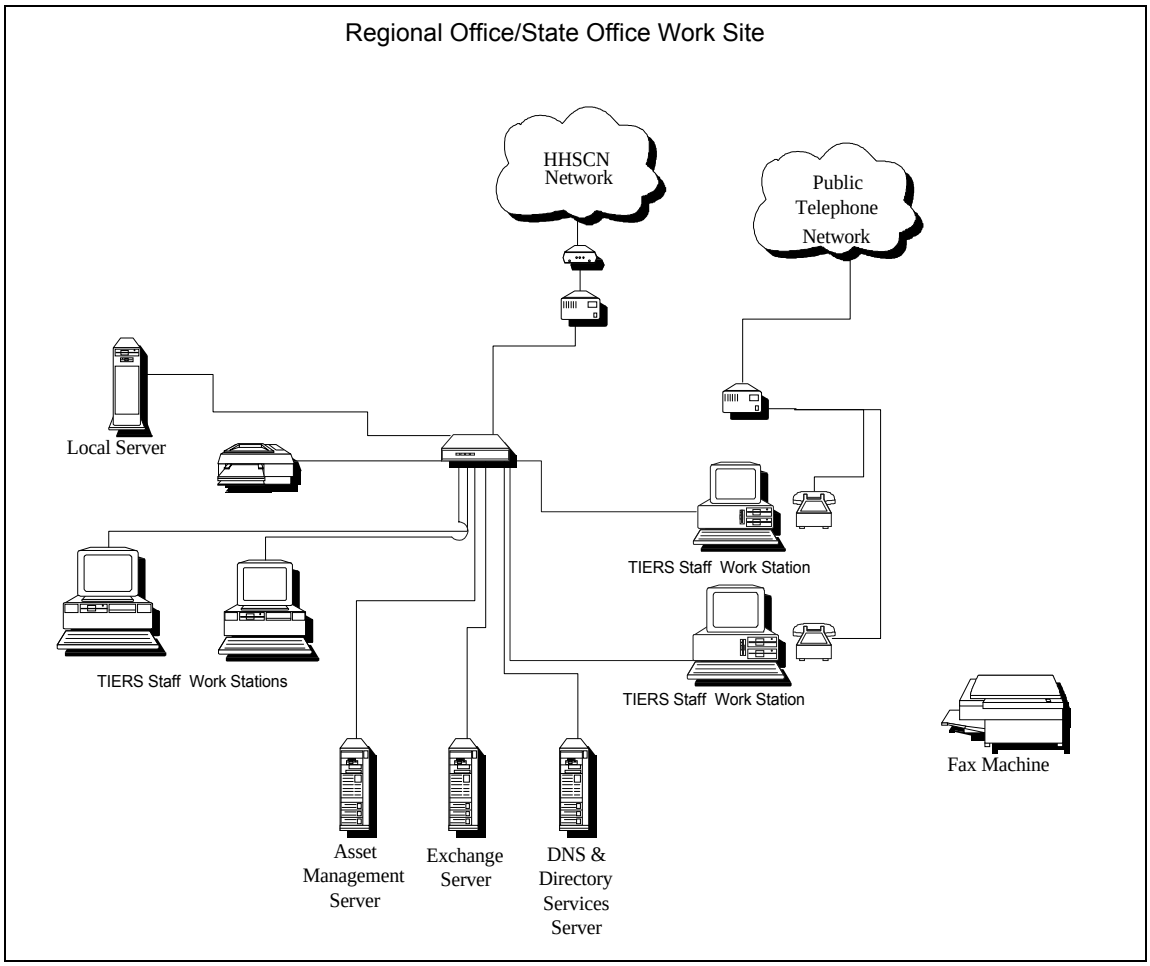


Figure 4 – Regional Office/State Office Work Site Configuration

The regional office/state office work site, as depicted in Figure 4, provides State staff with the tools and access needed to perform administrative and managerial tasks in support of the local offices. There are 10 regional offices across the state. Additional state applications will also be running on regional office desktop PCs in addition to the TIERS application.

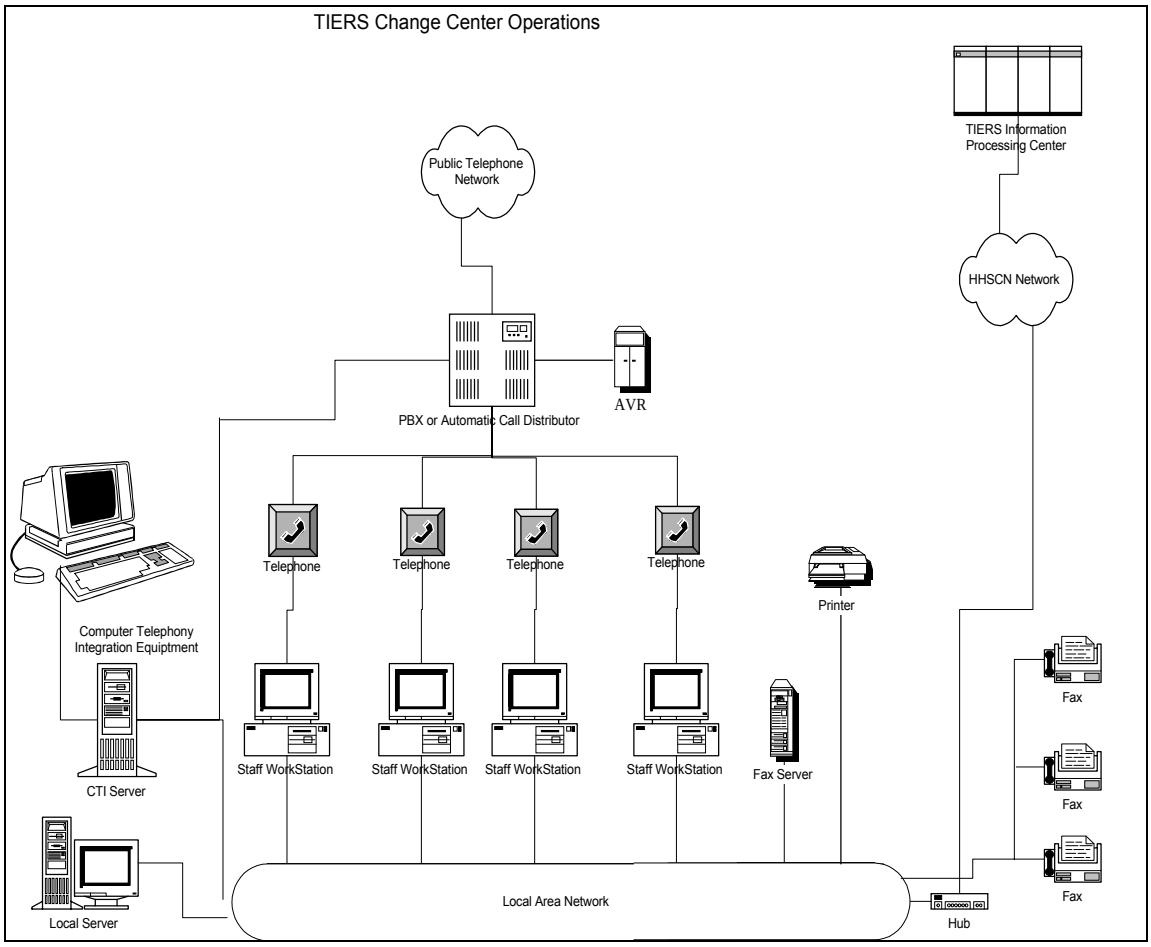


Figure 5– Change Center Configuration

The Change Center(s) will provide the client interface through the eligibility staff and perform tasks including accepting client changes and determining the affect of changes on client eligibility. Additionally, the center will be able to send/receive faxes, have local print capability, have access to the Internet and have access to client information to support daily activities. The Change Center configuration is depicted in Figure 5.

Application Architecture

The vendor must identify their proposed application architecture. Significant components of an application architecture are identified and discussed in the following section.

All functionality provided by application software can be viewed as falling into one of five classes:

- Presentation Management - Presentation is the human-machine interface.
- Business Rule Enforcement - The business rules are the statements of policy which govern:
  - ⇒ Enforcement of contextual data validation not addressable via data item characteristics and data structure definitions found in the data dictionary
  - ⇒ Eligibility Rules that support the determination and levels of eligibility
  - ⇒ Determination of the software component to which control will be passed under specific conditions
- Data Validation - Data validation functions ensure that data values input through a presentation medium are appropriate prior to their use in business rule enforcement or storage/deposition in shared databases.
- Data Access - Data access focuses on retrieving data from the data structure.
- Process Control - Process control is unique in this list, in that it not only is a structural element within a program, it is the glue which governs the interaction among all other structural elements of an application.

These classes of functions, or elements of design as they are referred to during the software design process, serve as the initial criteria for partitioning of software during design and subsequent construction. Partitioning of software by function in this model may result in a single software component to provide functionality in all classes or a number of software components for each class.

In an effort to reduce the complexity and number of business rules associated with TIERS, the agency is embarking on a policy consolidation process. This consolidation will reduce the total number of business rules that exist today to a more manageable number as well as take steps to apply consistency to policy across all TIERS programs. It should also be noted that the vendor is responsible for implementing this rule set into the overall TIERS application. The State anticipates a system which would allow centralized management of the rule set with ease of update, deletion and addition of new rules as it becomes necessary. *The vendor should describe in detail the proposed application architecture.*

Existing Applications

There are several applications within the State's portfolio which represent recent or ongoing investments. The State's strategy for these applications is to have the

TIERS vendor interface with these systems in the near term while developing TIERS functionality for the other in-scope programs. The interface with these systems will allow data entered into one system to be used to populate fields on the other, eliminating duplicate data entry. The applications in this category include, but are not limited to, the following:

- Lone Star Image System (LSIS) – Finger Print Imaging
- Electronic Benefit Transfer (EBT)
- Integrated Database Network (IDBN), a client registry system
- Client Assessment, Service Planning and Eligibility (CASE) system

Information Architecture

The data processing of an enterprise can easily be divided into three separate categories of systems. Each of these categories has, historically, its own set of users, processes, data sets, developers, technologies, and evolutionary paths. These three categories of systems are listed below:

- Definitional - This category contains systems which support the definition of the enterprise, including the acquisition, access and storing of knowledge about the enterprise.
- Operational - Operational systems are those which support the business of the enterprise, including the day-to-day activities at a detailed level.
- Analytical - Systems in this category support the enterprise itself, including the monitoring, evaluation, and redefinition of the day-to-day activities at an aggregate level.

This categorization impacts the information architecture in fundamental ways. Each of the categories of systems is so fundamentally different in nature that each resides in its own environment or domain. The data required to support each is likewise partitioned and allocated to the appropriate category. *The vendor is responsible for developing a system design consistent with the Information Architecture framework described above.*

Architecture Requirements

The vendor must propose a technical solution and select the technical components that meet the technical requirements specified in this document and the business requirements documented in the TIERS System Architecture Specifications, System Requirements Specifications and System Test Specifications. Following are additional guidelines that must be used in developing a technical solution:

- the ability to use the existing State network infrastructure and resources, leveraging the significant investment the State already has in place
- the ability for offices and agencies within the TIERS scope to operate continuously in the event of a system interruption within another office
- the ability to scale as case volumes grow or shrink and handle increases or decreases from the data source to the desktop with little effect on initially accepted response times
- the ability to interface to and share data with existing Legacy Systems during new system rollout
- the ability to perform multiple activities on the desktop within the TIERS system concurrently
- the ability to generate reports and provide ad-hoc information in a pre-defined time
- the ability to co-exist with other State agency applications residing on the desktop without creating configuration issues or response time issues
- the ability to open/close/move field offices on short notice with a minimum of expense due to technology installations

TDHS has spent considerable time defining the TIERS architecture. *The vendor must propose a n-tiered solution that conforms to the requirements and standards specified herein.*

B. Platform Standards and Requirements

Overview

It is the intent of TDHS to implement and maintain a set of technology acquisition principles and standards that will provide the appropriate level of computing resources to accommodate the processing needs at each tier in the enterprise. These standards are identified and maintained in the TDHS Enterprise Wide Technical Architecture. Should the existing standards require modifications, upgrades, or enhancements, the vendor will be responsible for documenting, justifying and proposing the changes to TDHS. The principles and standards documented in the Enterprise Wide Technical Architecture govern all TDHS projects. The standards documented in this architecture framework are TIERS project specific. The TIERS system must consider and accommodate these standards in the application design, development, and deployment phases of the project. This section of the architecture framework describes each of the required tiers of the system and lists the specific requirements for each tier. In addition,

Appendix B is a graphical presentation of the TIERS architecture that identifies the required functionality at each tier of the enterprise and lists the software standards for each tier.

The TIERS application system must interface with all legacy applications and data stores through interfaces defined in the TIERS System Architecture Specifications, System Requirements Specifications and System Test Specifications.

Technical Architecture Requirements

Hardware configurations proposed by the vendor must:

- be protected by an uninterruptible power supply that is capable of providing power to the servers for a period of no less that three hours.
- be in wide use and have a large installed base at the time of installation and be positioned for future upgrade.
- be configured to accommodate the current demand as well as support anticipated normal growth without requiring the purchase of a new machine.
- provide the ability for growth in CPU performance, memory, storage and I/O capacity.
- communicate with other tiers in the TIERS architecture.
- support bandwidth capable of meeting the TIERS business requirements.
- interface with a variety of network protocols through commercially available network interface cards (NIC).
- include the appropriate type of protocol stacks for the desktop and server to handle TCP/IP, which is currently implemented on existing State networks.
- have a significant number of vendors who are currently available to service the hardware.

Desktop

Standards

The Pentium-based Intel PC platform is the desktop standard. TDHS has an intent to establish a strategy that aggregates desktop requirements into groupings, such as low, medium and high platforms. The TIERS application will utilize a medium

platform for most processing requirements. TDHS is avoiding platform technologies and proprietary systems that do not have a broad installation base. TDHS will be providing all desktop hardware for the TIERS project, either through the use of existing hardware or the procurement of new hardware. *If the vendor requires a desktop configuration that exceeds the capabilities of the TDHS standard configuration, then the vendor must recommend upgrades to the TDHS standard configuration and provide a justification for the recommended upgrades.*

Requirements

Desktops will:

- consist of an Intel or compatible 32-bit microprocessor or better, running a 32-bit or better operating system.
- provide memory, storage, and I/O expandability once the minimum configuration for the proposed application is met.
- include a color monitor, keyboard and pointing device, and be Energy Star compliant.
- comply with the applicable ISO standards for emission and eyestrain.
- be a machine minimum configuration that represents the current market mid-point for PCs at the time of **installation**. (The PCs should neither be low-end or high-end, but be at the mid-point of performance in the market.) The rationale for requiring a market mid-point is that the State requires the application "foot print" to be as small a possible, thereby not requiring extensive processing to occur at the desktop level. The current TDHS standard for Desktop hardware can be found in Appendix A of this document.
- be configured with a common operating system, browser, word processor, Email client and anti-virus software. The current standards for each of these products can be found in Appendix A of this document.

Laptop

Standards

The Pentium-based Intel PC platform is the laptop standard. TDHS is avoiding platform technologies and proprietary systems that do not have a broad installation base. TDHS will be providing all laptop hardware for TDHS staff, either through the use of existing hardware or the procurement of new hardware. *If the vendor requires a laptop configuration that exceeds the capabilities of the TDHS standard configuration, then the vendor must recommend upgrades to the TDHS standard configuration and provide a justification for the recommended upgrades.*

Requirements

Laptops will:

- consist of an Intel or compatible 32-bit microprocessor or better, running a 32-bit or better operating system.
- provide memory, storage, and I/O expandability once the minimum configuration for the proposed application is met.
- comply with the applicable ISO standards for emission and eyestrain.
- be a machine minimum configuration that represents the current market mid-point for laptops at the time of **installation**. The current TDHS standard for laptop hardware can be found in Appendix A of this document.
- be configured with a common operating system, browser, word processor, Email client and anti-virus software. The current standards for each of these products can be found in Appendix A of this document.

Workgroup Servers (Specialized Servers)

Standards

This class of servers provides specialized services across the TDHS enterprise such as DNS, DHCP, Directory services, Exchange, NDS and/or ADS, Boot P, internet gateway, file and print services, and messaging services. These servers are configured to run the Windows NT, Linux and/or Novell operating systems. The PC-based servers must provide multiple expansion bays and SCSI/PCI based interfaces. The vendor can use existing workgroup servers when the functionality provided by server is required for the TIERS application. *If the vendor requires additional workgroup servers or additional services that are not currently available, they must provide recommendations and justification for those requirements.*

Requirements

Workgroup Servers will:

- consist of an Intel or compatible 32-bit microprocessor or better, running a 32-bit or better operating system.
- provide memory, storage, and I/O expandability once the minimum configuration for the proposed application is met.

- provide built-in fault tolerance capability.
- include a color monitor, keyboard and pointing device, and be Energy Star compliant.
- comply with the applicable ISO standards for emission and eyestrain.
- communicate with other tiers in the TIERS architecture.
- support RAID technology and internal and external tape storage requirements.

Note: Information concerning the current TDHS standards and products for workgroup servers can be found in the TDHS Information Systems Architecture.

Application Servers

Standards

Agencies housing large data stores or transaction-intensive applications are moving towards symmetrical multiprocessing or massively parallel multiprocessing solutions running UNIX or Windows NT. These hardware platforms are either RISC or Intel based. There will be 1 to n of these servers. In the future, an increase in the proportion of Intel-based servers is anticipated though they may be running UNIX. Server configurations must be POSIX-compliant and OPEN branded. The current standards for servers and server OS are listed in Appendix A of this document.

Requirements

Application Servers must:

- Consist of an advanced architecture that can support the requirements for high volume transaction processing.
- Provide memory, storage, and I/O expandability once the minimum configuration for the proposed application is met.
- Be upgradeable and scaleable.
- Provide built-in fault tolerance capability.
- Comply with the applicable ISO standards for emission and eyestrain.
- Tolerate power-supply failures with no system disruption.
- Provide redundancy to protect against cooling system failures.

- Provide service to most components while the system continues to run.
- Predict system failures through an integrated system monitor software.

Enterprise Servers

Standards

In the TIERS architecture this class of server will support the enterprise wide relational data base management system. There will be from "1 to n" of these servers running Oracle database in support of the TIERS application. *The vendor must propose a recommended configuration for the enterprise server(s) and provide an explanation of how the server(s) will be utilized.* The current standards for servers and server OS are listed in Appendix A of this document.

Requirements

Enterprise Servers must:

- Have a large user/installation base.
- Provide the ability to scale up and scale down as needs change.
- Tolerate power-supply failures with no system disruption.
- Provide redundancy to protect against cooling system failures.
- Provide built-in fault tolerance capability.
- Predict system failures through an integrated system monitor software.

Operating System

Standards

The TIERS System Architecture proposed by the vendor must use the current OS standard for Desktop, Laptop and server platforms as specified in Appendix A of this document. TDHS is avoiding proprietary and aging operating systems because of lack of support in the vendor community. The following standards apply to the operating systems in the TIERS architecture:

POSIX Compliance***:*** POSIX is the term applied to work produced by the Portable Applications Standards Committee (PASC). PASC is sponsored by the Computer Society of the IEEE (Institute of Electrical and Electronics Engineers) in the United States and is delegated responsibility for creating US National Standards in

the area of open systems. Operating systems must be POSIX-compliant which is reflected in documents ISO/IEC 9945-1, FIPS PUB 151-2 and IEEE P1003.2.

OPEN "Branded": Operating Systems must also be X/OPEN branded meaning compliant with X/OPEN Portability Guide, Issue 4 (XPG4).

UNIX "Branded"***:*** UNIX Operating Systems must carry the X/OPEN UNIX brand which represents the Single UNIX Specification also known as Spec 1170. This specification is a collection of documents that are part of the X/Open Common Applications Environment (CAE), and include: System Interface Definitions Issue 4, Version 2 (XBD), System Interfaces and Headers Issue 4, Version 2 (XSH), Commands and Utilities Issue 4, Version 2 (XCU) , Networking Services Issue 4, X/Open Curses Issue 4 Version 2. Compliance with this standard will provide smoother application portability and interoperability between 64-bit UNIX operating systems.

Requirements

Operating systems must be able to be upgraded without any changes in host hardware. Operating Systems must provide the following basic services:

- Access to hardware devices through an interface between a user and computing hardware
- Resource allocation ability
- Ability to select jobs or tasks that are to be dispatched through scheduling
- Ability to access data, perform or monitor the storage of data, and control input/output operations through data management
- Ability to mount and initialize various type of media through peripheral management

Printers

Standards

Printers will be used in the local offices, change centers, regional offices and state office to print reports, email, screen prints and client notices. The volume of the client notices will be high. The TIERS system must use existing agency printers if the printer satisfies the requirements for what is to be printed. *If the vendor proposes a solution that requires print capability above existing TDHS capabilities, the vendor must specify the printer configurations and provide justification for their use.* Existing printer types include laser, ink-jet and bubble jet printers for desktop solutions, line printers and dot matrix for character-based

printing needs. Printers must provide multiple paper feeding using a paper store of tray attachment and must have the ability to connect to the network through a network interface card and be IP addressable utilizing a print spooling mechanism such as Line Printer Daemon (LPD) protocol.

Requirements

Desktop printers must support the following:

- Graphics printing tasks such as image rotation and shading
- The 95-character ASCII subset
- Portrait and landscape formats
- Various styles and fonts for both landscape and portrait mode

C. Software/Application Standards and Requirements

Overview

This section outlines standards, guidelines and methodologies and also defines general requirements for the areas of Software Life Cycle Methodologies, Software Configuration Management, Commercial Off-The-Shelf Software Development Tools, Application, Middleware, Commercial Off-The-Shelf Application Software, Internally Developed Software, Presentation Style, Knowledge Transfer, Turnover, Reporting and Internet/WWW/Intranet.

Software Life Cycle Methodology

A set of defined repeatable processes is essential in addressing information system requirements in the enterprise business environment. The vendor and TDHS will agree on a proven methodology that has been implemented by the vendor on projects similar to TIERS. *The vendor using their methodology must provide a historical record of achievement.* The entire methodology must be accessible to the State agencies, and must describe tasks and deliverables and demonstrate metrics to measure the project's progress. *Preference will be given to vendor(s) that are SEI assessed at Capability Maturity Model (CMM) Level 2 or above.*

Standards

The vendor will be required to propose a life cycle methodology that is based on proven standards.

The vendor must provide documentation that describes the policies and practices of project management, including the following:

Quality Control Procedures: Description of the vendor's quality control policy and procedures including responsibility, top management oversight and audit procedures.

Planning and Tracking Methodology: Description of the vendor's proposed project planning and tracking approach and methodology, project reporting formats, and sample content must be provided. The progress reporting methodology must be keyed to the work plan element or milestones. It must also include the degree of completion and level of effort or resource expended for all tasks, work items and events and milestones identified in the work plan.

Change Control Methodology: Description of the vendor's change control methodology including sample logs, forms and reporting mechanisms and references on past use of the methodology including success rates, results and audits to support claims.

Any automation required supporting the QC, Planning & Tracking or Change Control processes must be provided by the vendor.

Requirements

The Software Life Cycle Methodology proposed by the vendor must, at a minimum, support the following:

Communication Processes - Define the communication processes by which the vendor will communicate project progress and quality adherence.

Inspectable Performance – Demonstrable, tangible evidence of process, progress and quality must be an integrated part of the methodology.

Reviews - Adequate, scheduled customer reviews of vendor performance based on milestones and time frames.

Issue Resolution - A process to be followed by the vendor to respond and, where appropriate, resolve findings generated by the reviews.

Technology Assignment - Assignment of a technology(ies) to each business process to be supported.

Requirements Management - Establish and maintenance of an agreement with the customer on the requirements for the application project. The agreement covers both the technical and non-technical requirements. This agreement forms the basis for estimating, planning, performing, and tracking the application project's activities throughout the project life cycle.

Modeling - Formal modeling of major alternative features of the technical design must be supported.

Construction - Construction of the software from coding to user acceptance testing must be included in the methodology.

Deployment/Implementation - Preparation for a successful application roll out with adequate support in such areas as testing, training, and technology deployment.

Ongoing Maintenance - A plan for managing the ongoing enhancement of the application until its retirement must be provided.

Transition - A plan for transitioning application support and operations to a third party or the State, in the event that it becomes necessary.

Legacy System Transition - An approach for moving from the legacy system to the new system must be accounted for in the proposed methodology.

Data Conversion - A process for converting existing, quality data elements into the new data structure must be included in the methodology.

Software Configuration Management

Standards

CA CCC/Harvest is the standard tool supporting both configuration management and life cycle control at TDHS. Both software elements and documentation are maintained in Harvest. *The vendor must propose a configuration management software solution that can be mapped to the standards in place at TDHS.* These standards are further defined in the TIERS Software Configuration Management Plan.

Requirements

The TIERS Software Configuration Management plan details the tasks, methodology, procedures and controls which will be used with the project.

Application

Standards

The vendor must propose a client/server application software solution that allows TDHS staff to correctly determine eligibility for all in-scope programs as well as

support verification, assessment, enrollment, benefit authorization, and referral activities. The solution should be flexible and scalable to accommodate TDHS transaction volumes. TDHS users should be able to access the GUI applications via desktop or a WEB browser. Priority will be given to products adhering to industry standards, open architecture, and have successful track records. *The vendor must implement an n-tier application solution.* TDHS' goal is to deploy many n-tier applications so that the potential for sharing common software services will be accessible from any user interface.

Additionally, the vendor must support transitioning of existing SAVERR, GWS and LTC worksheet application business rules to be incorporated into the TIERS application design and, ultimately, implementation. Note that an effort to simplify the business rules is currently under way.

Requirements

The Application Software must:

- Establish partitioning standards, allowing for direct systems development as well as ease of maintenance, portability and scalability.
- Minimize integration complexity through application design.
- Support seamless data access through a variety of interfaces.
- Design applications that are platform independent.
- Employ reusable components.
- Incorporate the ability to use standard middleware components.
- Use an industry standard WEB Browser that complies with the TDHS standard in Appendix A.
- Use technologies and products that are either Object-Oriented (OO) or are compatible with OO.
- Existing SAVERR, GWS and LTC worksheet business rules must be identified and implemented in the TIERS application. In addition, the on-going policy simplification process will modify existing business rules that must be incorporated in the TIERS application. Note that an effort to simplify the business rules is currently under way.

For more detailed information, please refer to the Application Section of the TDHS Enterprise Wide Technical Architecture document.

Middleware

Standards

The vendor must propose middleware software tool(s), which will provide transparent communication over multiple protocols and easily connect to a variety of data sources. The tool(s) will be the vehicle to provide asynchronous, event-oriented communication. The middleware must be commercially available and include warranty and software support.

Requirements

The software must:

- Use middleware that is independent of development tools.
- Use middleware that will support the design and implementation of event-driven systems.
- Allow TDHS security policies to control both data access and application access.
- Utilize products and vendors who adhere to industry standards and open architecture.
- Be compatible and support TDHS disaster recovery plan.

For more detailed information, please refer to the Middleware Section of the TDHS Enterprise Wide Technical Architecture document.

Commercial Off-The-Shelf (COTS) Software Development Tools

Standards

Off-the-shelf software development tools will be used in the design/development environment to develop the TIERS application. These development tools must be commercially available and include warranty and software support. *The vendor should include a description of their plan for incorporating and using design/development tools in the new development of, or transfer of an existing system, as well as the rationale for selection of the tool and its planned usage.* These tools may include, but are not limited to Ad Hoc reporting tools, Automated Test software, CASE tools, Visual software development tools, etc. All COTS Software development tools bought for this implementation will be subject to knowledge transfer requirements as described in the Knowledge Transfer section of this document. For more detailed information, please refer to the TDHS Information Systems Architecture and Enterprise Wide Technical Architecture documents.

Requirements

The COTS Development Software must:

- Provide a full range of functionality within a client/application server paradigm for applications with complex business rules operating on complex data structures.
- Support software specifications in a manner visual rather than textual, descriptive rather than procedural, and natural rather than cryptic.
- Support the creation of all windows presentation idioms.
- Support static and dynamic software analysis.
- Be compliant with industry standards for effecting interaction among software modules (such as DLL, DDE, and OLE).
- Interact with repository managers, data dictionaries, and configuration management utilities.
- Not maintain its own proprietary database.
- Result in well-partitioned software components of manageable size which use memory, mass storage and CPU efficiently.
- Accomplish server communications through SQL, RPC or transaction processing monitor.
- Have significant market share and be provided by an organization in good fiscal health.

TDHS' preferred transaction processing monitor (TP/monitor), Tuxedo or functionally equivalent product, will be used to manage two-phase commits and data access across platforms. TDHS' preferred application development environment, either IBM's WebSphere application server with the VisualAge IDE or BEA's WebLogic application server with the Visual Café IDE must be able to communicate with the Unisys mainframe and easily integrate with the TP/monitor.

It will be the responsibility of the vendor to provide the services to properly implement the development products in the TDHS environment and to provide direction and information regarding required training for TDHS staff who will support these products.

Commercial Off-The-Shelf (COTS) Application Software

Standards

Hardware-independent, off-the-shelf software packages should be used to satisfy requirements whenever possible to minimize the dependence on custom-developed software and reduce development and maintenance costs. The extent to which the vendor proposes to integrate COTS software will be a factor in evaluating the vendor's proposed solution. The vendor should refer to the Application Services Table in the TDHS Information Systems Architecture document to review the standard TDHS COTS Software. *If the vendor chooses to propose a COTS Software not on the TDHS list for TIERS implementation, the off-the-shelf software must be commercially available and include warranty and software support.* All COTS application software bought for this implementation will be subject to knowledge transfer requirements as described in the Knowledge Transfer section of this document.

The COTS Software user interface should comply with the Microsoft Style Guide for consistent look and feel across all applications.

An office software suite of tools represented by Microsoft Office has been chosen as the standard office suite for the desktop when applicable to the role of the user. COTS Software must not replace any of the existing office software suite functionality, and must integrate with the software via the commercially provided interfaces. COTS Software may not be modified.

Requirements

The COTS Applications Software must:

- Be compatible with the existing technical environment and future environment of TDHS programs.
- Be compliant with industry standards for effecting interaction among software modules (such as DLL, DDE, and OLE).
- Not maintain its own proprietary database.
- Have significant market share and be provided by an organization in good fiscal health.

Internally-Developed Software

Vendors may propose either new development or transfer and modification of existing systems that provide all or a portion of the functionality required by TIERS. The system shall provide all the functionality that TDHS staff needs to correctly determine eligibility for all in-scope programs. The system must meet or exceed the functional and technical requirements set forth in the procurement

document. The application should be adaptable to new functionality required to be compliant with any new federal or state law. *Vendors should minimize the need to manually perform data corrections/modifications but provide this functionality when necessary.*

Standards

Custom-developed software must be used where the functionality of COTS software does not meet the business or architectural requirements as defined in the procurement document. Guidelines and standards will be developed through dialog and written agreement between the vendor and TDHS.

Internally developed software will possess the following traits:

Portability. Internally developed software must adhere to Open Systems standards and must be portable, leading to increased ease of movement across heterogeneous computing platforms. Portable applications provide a smoother transition and reduced impact on operations as technological improvements occur to host platforms.

Scalability. Internally developed software must be configurable, allowing the application to be operable on the full spectrum of platforms required.

Reusability. Development of business independent modules where applicable must reduce the amount of software developed and add to the inventory of software suitable for re-use by other systems.

Maintainability. Internally developed software must be maintainable through the use of standards developed through the mutual understanding between the vendor and the State agencies. Standards must also be dependent on the coding language being used. Standards must include the following:

⇒ Software documentation standards

⇒ Naming conventions

⇒ Programming style

⇒ Program modularity

Requirements

Internally Developed Software `must:`

- Be partitioned by class of functionality as defined in the Application Section of the TDHS Enterprise Wide Technical Architecture document.

- Be able to execute under multiple tiers and be portable to each tier, if applicable. This system will be an n-tier application.

- Propagate changes to other tiers through automated tools without the need for re-coding through manual assistance or intervention.

- Have a small application footprint on the desktop device.

Presentation Style

Standards

A consistent user interface ensures that all user-accessible functions and services will appear and behave in a similar predictable fashion regardless of the application, business process or site. Internally developed software that incorporates the development of graphical user interfaces must follow established guidelines based on Microsoft GUI Standards. These standards are derived from Microsoft's The Windows Interface: An Application Design Guide.

All internally-developed user interfaces will be compared against a GUI Standards Checklist for compliance in such areas as standards and guidelines on interface consistency, navigation, user feedback, ease of use, input devices, presentation design, user messages, icons, use of color, and effective help. Any exceptions to the proposed GUI guidelines and standards when driven by business requirements must be documented in an exception report and include sign-off from TDHS.

Additionally, the vendor will use Bobby, a WEB based analysis tool, to analyze the TIERS WEB based application to ensure accessibility to people with disabilities and to comply with the Americans with Disabilities Act. TDHS supports ADA and wants to ensure people with disabilities can use TIERS.

Requirements

The Graphical User Interface must:

- Comply with or conform to the Microsoft Windows Application Design standards.

- Provide the ability to access and operate on any form of data within an individual window, independent of all other windows.

- Allow direct manipulation of screen elements.

- Support pointing devices to facilitate access and manipulation.

- Utilize standard visual control elements including icons, buttons, scroll-bars, menus, and dialog boxes.

- Maintain consistency across applications and platforms.
- Receive a "Bobby Approved" rating for its WEB based application site (http://www.cast.org/bobby).

System Documentation

Standards

System documentation will include the requirements, capabilities, limitations, design, operations and maintenance of TIERS both electronically and within user manuals. It is extremely important that the process models, user interfaces, user's guides and a TIERS data dictionary are documented to support problem isolation and resolution once the system is implemented. Processes must be documented, accessible, and repeatable in order to ensure that the business process of determining eligibility for potential clients will not be hampered long term.

Requirements

Complete system-level and module-level analysis as well as design specifications, data element/object dictionary, process models, user interfaces, and user's guides must be provided before implementation. Additionally, graphical representation of system modules, interfaces, internal/external dependencies, inter-process communications, and software layering must be provided. *The documentation provided by the vendor should accurately describe the system as implemented. The vendor is required to interface their document management processes with/into CCC/Harvest.*

Knowledge Transfer

Standards

Knowledge transfer refers to a style of consulting that places a premium on imparting the skills and knowledge of the Consultant (or vendor) staff to the State staff assigned to the project. The transfer of knowledge is accomplished through training (formal and informal), mentoring, and actual hands-on participation. There are not any industry standards associated specifically with knowledge transfer. However, many vendors have developed methods for accomplishing skill and knowledge transfer. The objective of the TIERS project is to accomplish skill and knowledge transfer by a vendor who has proven experience on a large complex system's project like TIERS. Beyond the knowledge transfer requirements, the vendor will need to adhere to documentation requirements described in the Turnover section in this document.

Requirements

TDHS will require the vendor staff, in context of producing contract deliverables, to work collaboratively with TDHS designated staff throughout the project's life cycle to provide education on tools, deliverables and process development. Additionally, TDHS will require the vendor to provide a knowledge transfer plan including written objectives for different levels of TDHS staff and the different phases of the TIERS project. The plan should contain a strategy for accomplishing skills and knowledge transfer between the vendor and TDHS Staff including tools and methodology. The plan should also propose a method to measure the success of the knowledge transfer. There will be periodic reviews or status reports throughout the life of the project. These activities will allow TDHS to minimize cost and disruptions associated with change as well as capitalize on investments made in the TIERS initiative.

Turnover

Standards

The vendor shall turnover all operations and technical support in a low-risk, orderly, and transparent as possible transition to TDHS or new vendor upon notice of contract non-renewal or termination.

Requirements

TDHS responsibilities for turnover are:

- Approving the vendor's turnover plan; and
- Coordinating turnover activities.

The vendor's responsibilities for turnover are:

- Planning, data and software migration, and documentation transfer. The turnover shall include all state-owned databases, data structures, data, systems, and programs; and documentation including diagrams, flow charts, data maps, and other information necessary to assist TDHS or the new vendor in understanding and re-establishing successful operation of the system being transferred;
- Provide all final licensing agreements on proprietary products to support TDHS' or the new vendor's usage following contract termination;
- Provide a thorough list of all logins and passwords on any system or computer belonging to the state;
- Submit turnover plan six (6) months prior to the end of the contract; and

- Include turnover activities within submitted bid price.

Reporting

Standards

TDHS staff will be able to use reporting tools to perform queries and analysis as well as display eligibility information contained within TIERS either online or in a printed format. The TDHS staff will be able to write queries and generate reports without the assistance of any technical staff. They will be able to access, produce, and research reports that will assist them in performing their normal day-to-day responsibilities.

Requirements

Numerous reports required to support TIERS must be generated at both local and centralized locations. These include, but are not limited to, federally mandated reports, month-end reports, statistical reports, and case management reporting, internal management reports, and ad hoc reports. Users must be provided access to these reports via on-line display from their individual workstation. Report retention and printing options will be determined separately.

Internet/WWW/Intranet

Standards

The 1997 version of the State DIR Strategic Plan for Information Resources Management provides a mission and vision along with additional goals and objectives for the use of technology and provision of public services for the people of Texas. In support of these initiatives, DIR SRRPUB11, World Wide Web Design and Coding Guidelines, addresses the use of the World Wide Web as a means of facilitating public access to government information and services.

DIR SRRPUB11, World Wide Web Design and Coding Guidelines can be found at http://www.state.tx.us/Standards/srrpub11.htm.

Requirements

The Internet/WWW/Intranet must:

- Allow Internet access for desktop environments dependent on the business need. This may include, but is not limited to, Internet access software, browsers, communication software, security software and e-mail interface.

- Integrate into the TIERS application, but remain separate from the existing network and data.

- Provide monitoring tools to monitor usage.

D. Network Architecture/Telecommunications Standards and Requirements

There are two basic types of networks used by TDHS: Local Area Networks (LANs) and Wide Area Networks (WANs). It is the appropriate combination of LANs and WANs, plus the networking protocols, that form the basic communications infrastructure for TDHS. It is the intent of the agency to implement and maintain a set of principles and standards that specify how information processing resources are interconnected, and documents the standards for protocols (for network access and communications), topology (design of how devices are connected together), and wiring (physical medium or wireless assignments). These standards are identified and maintained in the TDHS Enterprise Wide Technical Architecture. The TIERS system must consider and accommodate these standards in network design and implementation. In addition, the TIERS system must utilize the following network resources: TDHS LANs, HHSCN, and TEX-AN 2000. Each of these resources will be discussed in more detail on the following pages.

Local Area Network

Standards

Topology

TDHS LANs consist of a diverse mix of 10/100 Mb Ethernet, 4 and 16 Mbps Token Rings, and FDDI. Ethernet switches are the preferred concentrators for locations with more than 10 workstations. Ethernet and Fast Ethernet will ultimately replace Token Ring as the primary local area physical layer.

Protocol

TDHS is currently standardizing on the TCP/IP. *The vendor must propose the appropriate type of protocol stacks for the desktop and server to handle TCP/IP, which is currently implemented on existing State networks.* The TDHS technology policy is to avoid IPX protocol.

Cabling

The Texas HHS cabling standards are based upon the EIA/TIA (Electronics Industry Association/Telecommunications Industry Association) 568, 569, and 570 Commercial Building Telecommunications Wiring Standards. The General Services Commission (GSC) and the Department of Information Resources (DIR) also specified these standards as the cabling standard for all new State structures and State structure renovations.

The EIA/TIA standards define generic voice and data telecommunications wiring systems that will support multi-product, multi-vendor, and multi-topology environments. Adoption of these standards allows TDHS to establish a premises wiring system without requiring prior knowledge of the telecommunications products or topologies that will be installed at the site.

Cabling standards documentation can be found at http://www.mhmr.state.tx.us/hhscnet/premises.htm.

Requirements

- To the extent possible, the vendor must use the TDHS current LAN infrastructure.
- The vendor and agency infrastructure experts must study each LAN environment and, if required, recommend additional components and or modifications to the existing environment necessary to support the proposed design. If changes are required, the vendor must provide a justification for the additional components.
- Changes to LANs must not affect sites with LANs supporting multiple agencies, of which some do not require a TIERS application.

Wide Area Network

Standards

The TIERS system will be required to use the HHSCN. The HHSCN will evolve over time and may one day provide a common statewide backbone. There are several external factors that may impact the HHSCN in the future and which should be considered in TIERS design. These are Senate Bill 365, of the 75th Legislature; House Bill 2641, of the 76th Legislature; and the TEX-AN 2000 project.

Senate Bill 365 establishes the Telecommunications Planning Group (TPG). This group's primary role is to develop a statewide telecommunications plan that will move Texas network(s) into the 21st century.

Additional information on the role of the TPG can be found at http://www.state.tx.us/TPG.

House Bill 2641, of the 76th Legislature, states that HHSC is responsible for strategic planning for information resources at each health and human services agency and shall direct the management of information resources at each health and human services agency.

The TEX-AN 2000 project is discussed later in this section.

Requirements

The Wide Area Network must:

- Provide application performance data and anticipated bandwidth requirements for the proposed design.
- Use current network utilization and capability data along with estimated requirements to support any design decision.
- Be modeled using a software tool (e.g. SES-Workbench and/or SES-Strategizer) by the vendor at projected peak transaction volumes and caseloads to ensure performance levels will be met and excess capacity is available. The vendor is required to maintain this model based on actual performance and have the model periodically evaluated by agency Subject matter experts. TDHS will make current network utilization information available to support this effort.
- Incorporate any suggested or required modifications, that are approved by HHSC, to existing backbones is the responsibility of TDHS and or backbone service provider. These modifications must balance cost against performance.
- Consider current Internet access requirements and TIERS HHSCN interface requirements and make IP management recommendations if necessary.
- Retain network management functions as the responsibility of the respective network administrators and member agencies. Hardware dedicated to TIERS proposed by the vendor and agreed upon by the agency must be manageable by industry standard protocols such as those referenced in the TDHS Enterprise Wide Technical Architecture.

HHSCN

The Texas HHSCN is a statewide telecommunications cooperative between State agencies and private enterprise that connects and manages networks from the data center to the desk top. Governed by a board of its constituents, the partnership was originally created by the HHSC to share network costs and services among the 11 Texas HHS agencies. Since its inception in September 1994, the HHSCN has extended its services to other entities, including State agencies outside of the HHSC, organizations outside of State government, and even organizations outside the state of Texas.

The HHSCN backbone consists of 12 nodal sites in a fully redundant configuration with the eventual goal of one nodal site in each LATA (see Figure

6). The backbone carrier is dedicated T1. Inter-node link utilization is monitored and bandwidth added if necessary. Most local sites connect through fractional T1 leased lines. Local leased lines are being transitioned to ISDN where cost effective and where disaster recovery is critical. HHSCN traffic consists of TCP/IP, IPX and SNA.

A more detailed description of HHSCN can be found at http://www.tx.net.

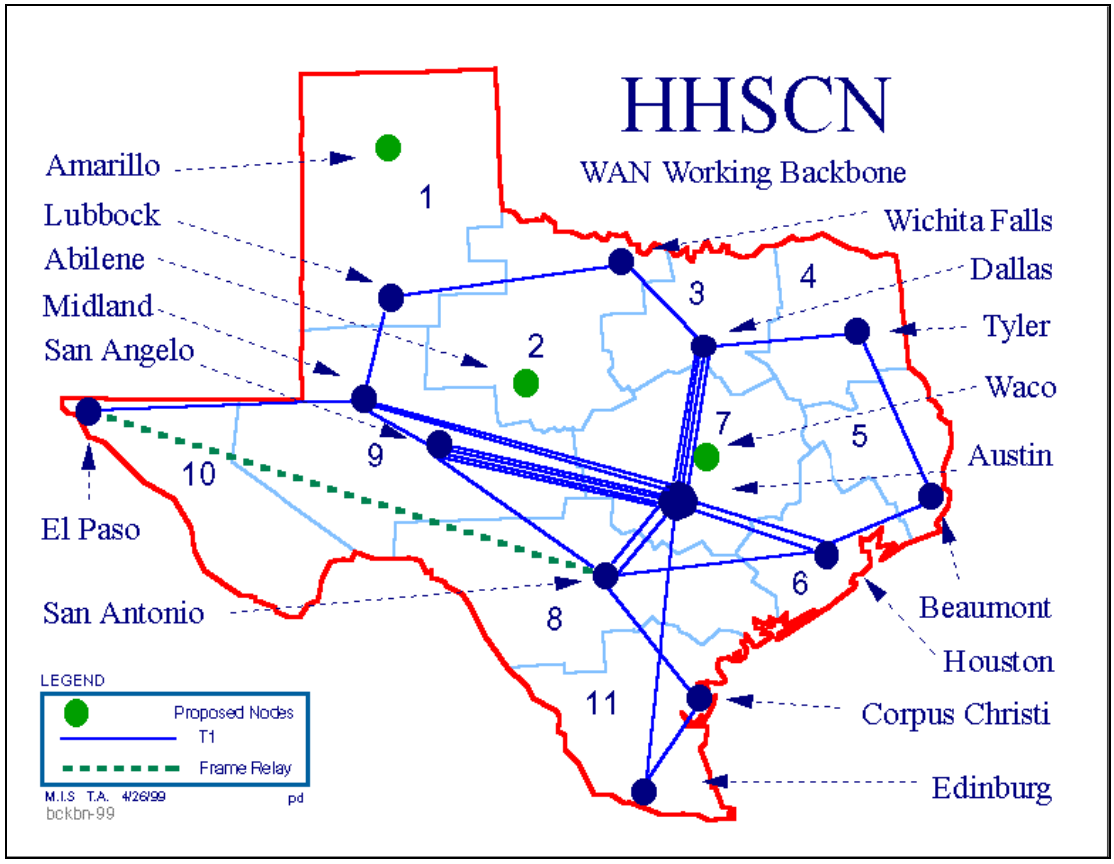


Figure 6 – HHSCN Backbone (http://www.tx.net/maps/backbone.htm)

The Internet gateway is provided by the Greater Austin Area Telecommunications Network (GAATN). The GAATN is a joint effort of the Austin Independent School District (AISD), Austin Community College (ACC), City of Austin, Lower Colorado River Authority (LCRA), Travis County, The State of Texas represented by the State General Services Commission and The University of Texas at Austin that constructed a metropolitan-wide information super-highway. It supports Token Ring, Ethernet, FDDI, Sonet and ATM connections between participants' sites and also provides high speed Internet data routing.

A more detailed description of the GAATN can be found at http://www.gaatn.org/.

Telephony

Standards

TDHS currently has an installation base of primarily Nortel telephony hardware for their infrastructure components.

Requirements

The vendor must utilize the existing equipment install base to the extent possible. Any solutions, which do not utilize the existing infrastructure, must include substantial rationale for not doing so.

TEX-AN will provide all inter-city voice service. *Using current TEX-AN rates and TIERS business requirements, the vendor must develop a cost effective change center placement strategy consistent with TIERS business needs.* This strategy must consider leading edge technologies such as voice over IP to minimize long distance costs, if practical. WAN backbone abilities should also be considered in any alternative telephony design.

Additional information about TEX-AN and its current service offering can be found at http://www.tex-an.net.

Naming Conventions

Standards

The HHS addressing and naming conventions standards were adopted by the HHS Telecommunications Workgroup to ensure that all HHS agencies have consistent access to the HHSCN. Using the HHS addressing and naming standards is required in order for an agency to participate on the HHSCN.

Server

Server naming standards have been developed by the HHS agency and can be found at http://www.mhmr.state.tx.us/hhscnet/library.htm.

Personal

Vendors are required to be compliant with DIR SRRPUB10, Electronic Mail Personal Naming Convention. X.400/Internet Personal Naming Recommendation defines a uniform naming format that allows users to be addressable by a minimum set of address elements. Every electronic messaging user must be addressable by at least their Given Name, Initials and Family Name, irrespective of the messaging system they are using. The "Personal Naming Convention" is based on the existing standards for e-mail exchange and directories (Simple Mail

Transfer Protocol (SMTP) and Lightweight Directory Access Protocol (LDAP) or X.500 Directory Services).

DIR SRRPUB10, Electronic Mail Personal Naming Convention can be found at http://www.state.tx.us/Standards/srrpub10.htm.

Requirements

The vendor must work with TDHS to recommend naming conventions which will serve the needs of all participants. This includes, but is not limited to, servers and personal naming conventions.

E. Data Standards and Requirements

Overview

This section outlines standards and defines general requirements for the areas of Relational Database, Distributed Database, Data Access, Data Warehouse, Data Modeling, Referential Integrity, Data Retention, Information Exchange, Systems Development, System Test , User Test and Training Environments, and Disaster Recovery Plan.

Relational Database

Standards

Data stores must operate independently from applications, network environment and platform, and must be designed for consistency, standard access and optimal performance. The Data Base Management System (DBMS) must include security, data integrity, and provide data rollback functionality.

The Structured Query Language (SQL) chosen should conform to the American National Standard Database Language SQL, ANSI X3.135-1992.

Requirements

Relational Database Management System must possess the following attributes:

- Multi-threaded client application support
- Unlimited database size
- Scalable, parallel architecture
- Both intra-partition and inter-partition parallelism

- Parallel sorts, joins, and aggregates
- Parallelization of PL/SQL functions
- Scalable SMP performance
- Queuing with publish and subscribe model
- Solution for high availability requirements
- Online backup by file, tablespace, or database
- Mirrored multi-segment log files
- Secure, remote database administration
- Full transactional consistency and data integrity
- Transparent remote and distributed query
- Transparent, multi-site distributed transactions
- Failover configuration support
- Choice of internal or external user authentication
- Password policy enforcement
- Global users and roles
- Encrypted passwords
- n-tier authentication/authorization
- Automatic auditing on per-session or per-object basis

Distributed Database

Standards

Distributed database systems usually provide greater throughput and higher availability than single physical or logical central servers. Distributed databases can be used to implement TIERS if the vendor chooses to propose it as a solution. The database may be logically distributed or reside on multiple boxes but primary database is not expected to be distributed to local sites.

Requirements

If the vendor chooses a distributed database design then the design must:

- Permit each office to continue operating TIERS regardless of the status of another office's database status.

- Redundant data must be synchronized automatically, following the completion of a logical unit of work. Under the TIERS architecture a logical unit of work is defined as a task or group of tasks that cause a change to the data source when completed. For example, this could be done through publish and subscribe or a two-phase commit.

Data Access

Standards

Standard public Application Programming Interfaces (API) must be used as the data access standard. Information must be managed through a data agent and must not be initiated through the application via embedded SQL. APIs must incorporate the Open Group's Call Level Interface (CLI) which is included in both native and ODBC drivers. There will not be any direct access to the data from the client to the server. The data must always be accessed through the middleware software.

Requirements

A metadata repository and a data dictionary with TIERS data must utilize the same definition for data format and content to ensure that statewide information reflects consistency in its definition and understanding.

The vendor must work with all programs within scope to determine the best way to:

- Support information exchange as it is currently shared across programs;

- Maintain comprehensive financial and categorical information in the TIERS automated system;

- Make financial and categorical information available to other programs for the purpose of administering programs; and

- Demonstrate how clients will be assured of their right to confidentiality.

Data access must:

- Be executed independent of platform;

- Be executed through a data agent and not directly through an application; and

- Retrieve only information from the data source initiated by an authorized requester that is relevant to the requester.

For more detailed information, please refer to the Data Management Section of the TDHS Enterprise Wide Technical Architecture document.

Data Warehouse

Standards

The vendor will propose a data warehouse to facilitate the business reporting requirements of TIERS. The primary purpose of this application environment is to provide decision-makers with the information they need to make informed decisions. Enterprise data is manipulated and presented in such a way that it "becomes" information. Published international standards for a data warehousing architecture do not exist at this time.

Requirements

The central features of the data warehouse will include:

- Computer analysis of TIERS data using Online Analytical Processing (OLAP).
- Discovery and extraction of information using data mining tools.
- Extraction, transformation and cleansing of operational for preparation and loading into the data warehouse.
- Software tools that enable business users to see and use large amounts of complex data. The tools provide ad hoc query, canned or structure reporting, graphical, trend analysis, and summarization capabilities.

The amount of data transferred is significant enough that the connection(s) between these two environments warrant special attention.

For more detailed information, please refer to the Data Warehousing Section of the TDHS Enterprise Wide Technical Architecture document.

Data Modeling

Standards

All database development in the TIERS Architecture must begin with a data model. Data must be partitioned into subject areas rather than by business or departments. The vendor and TDHS will agree on a proven methodology for the creation and documentation of the data model. Logical data models must be developed and normalized to the third normal form. Standards must also be

developed to document any denormalization of the physical and analytical models. Data stores must be normalized across the enterprise. *The data modeling methodology proposed by the vendor must be integrated with the overall system development methodology.*

Requirements

Data Modeling must be performed using an automated tool that:

- Provides the definition and enforcement of data integrity
- Converts from a logical to a physical model
- Creates a physical schema
- Supports an industry accepted modeling methodology

The vendor will provide a tool that enables database developers and administrators to create models at all necessary levels of abstraction to analyze information needs and transform them into database solutions. This includes meta models for the repository as well as models for OLTP and OLAP logical and physical databases. Use the same tool for modeling at various levels and for different databases (i.e. provide tight coupling among enterprise level information models, logical data models, physical data models, and transform functions to create key physical database components, regardless of the database target environment). Approved tools must support UML. Approved tools must be capable of storing all modeling items.

Referential Integrity

Standards

The relational data model must include functionality to enforce referential integrity. Declarative referential integrity applies to the mechanism by which the RDBMS maintains associated relationships in multiple tables.

Requirements

Referential integrity must be enforced by the RDBMS where it makes sense in the design and does not impede performance. An alternate solution to maintain integrity must be designed in the latter situations.

Data Retention

Standards

The vendor must comply with TDHS' data retention standards based on the business requirements and established federal data retention requirements on a program by program basis.

Requirements

- Audit trails must be available for user and system initiated actions for all add, update and delete transactions. The audit trail must be available for on-line inquiry for a duration to be determined by the TDHS and no modification will be permitted to audit trail data.
- Audit trails may be stored off-line on a machine-readable media after the on-line requirement has been met.
- TIERS must supply a date and time snapshot display of all data for audit and verification purposes. The system must display information used to determine verification, assessment, determine eligibility, enrollment, and referral activities. A history of data elements must be maintained.
- Application data update needs/frequencies will be identified.

Information Exchange

Standards

Two types of information exchange are described in this section: first, the information exchange that occurs via e-mail correspondence and second, information that is exchanged in bulk with the agencies' various data trading partners.

Requirements

Electronic Mail

Vendors are required to be compliant with DIR SRRPUB12. This publication addresses standards for e-mail systems and document interchange between and among State agencies and the public. SRRPUB12 Information Exchange Standards can be found at http://www.state.tx.us/Standards/srrpub12.htm. The TDHS software package requirements for Information Exchange are documented in Appendix A.

Bulk Data Exchange

Bulk data exchange is a complex issue involving numerous agencies and systems. Currently, there is no standard for exchange interface or media. Today, magnetic tape comprises a significant amount of the data transfer. Numerous electronic transfers also occur. File Transfer Protocol (FTP) is preferred for electronic transfers. Exchange mode is determined by data size, transfer time and/or network bandwidth. The vendor is responsible for developing interfaces with the numerous systems including other TDHS organizations and external Agencies. If the files transferred are within agreed upon constraints of size, time and bandwidth, electronic transmission of the data is required. For files that are too large, a media, such as magnetic tape, may be used to transfer the data to the trading partner. Given the large number of interfaces, it is the State's goal to generalize the transfer process rather than developing unique code that is not re-useable for other interfaces. Interface requirements must be defined for each system and passed as arguments to an interface layer. All interfaces (internal/external) will be documented incorporating the following elements:

- Record description/data items;
- Volume;
- Frequency;
- Retrieval/update;
- Backup/recovery; and
- Media/transport.

Systems Development, System Test, User Test and Training Environments

Standards

The vendor must have separate systems development, system test, user test (which will follow the TDHS Model Office Automation testing initiative procedures) and training environments. There will be a varying range of data within each environment dependent upon the unique needs of the different life cycle phases. *The vendor must purchase systems development and testing tools that will be able to import original requirement documentation from analysis through implementation phase of the TIERS project.* These testing tools should perform automated and manual testing including, but not limited to, regression, load, stress, performance, object, event, and field as well as store the results in an administered repository structure.

Requirements

The requirements for systems development, system test, user test (*which will follow the TDHS Model Office Automation testing initiative procedures*) and training environments are identified below:

- Provide separate environments for systems development, system test, user test *(which will follow the TDHS Model Office Automation testing initiative procedures*), and training areas.
- Perform functional testing, load testing, and performance testing prior to the TIERS implementation.
- Provide statistical results of functional testing, load testing, and performance testing completed prior to the TIERS implementation; TDHS sign-off required.
- Provide security authorization for each environment (systems development, system test, user test and training) by individual user including vendor and TDHS staff.
- Provide training (formal and informal) as well as mentoring on both data as well as TIERS.

F. Security and Confidentiality of Information

Confidentiality

Confidential information must be accessible only to personnel who are authorized by the owner on a strict "need to know" basis in the performance of their duties. Data containing any confidential information must be readily identifiable and treated as such in its entirety. When confidential or sensitive information from one agency is received by another agency in connection with the transaction of official business, the receiving agency must maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency.

Standards

State and federal law regulate maintaining the confidentiality of client information through such laws and regulations including, but not limited to, the Food Stamp Act (7 U.S.C. Section 2020(a)(8)), the Social Security Act (42 U.S.C. Section 1396(a)(7)), Internal Revenue Code (26 U.S.C. Section 6103), the Texas Human Resources Code (Section 12.003), and the Texas Public Information Act (Tex. Government Code, Chapter 552). Compliance with these regulations can be accomplished by using a restricted level of security in computer systems.

Requirements

TIERS must be constructed to maintain client confidentiality in accordance with the requirements applicable to information relating to applicants and recipients of public assistance under State and federal law.

Security

Texas Administrative Code 201.13(b) requires that each agency identify, classify and protect the automated files, data bases and applications for which it has ownership responsibility. Classifying information and the applications that function to process it is at the heart of identifying and selecting appropriate security and risk management practices. Each agency's security objectives must include maintaining information integrity and confidentiality and assuring the availability of critical information technology support services.

Standards

The following DIR web page contains the required minimum security standards for the protection of automated information resources for agencies of the state of Texas. These standards are available at http://www.dir.state.tx.us/IRAPC/StdsF2.html.

Additionally, TIERS must follow the security standards as defined by the following publications, but not limited to:

- Automatic Data Processing Physical Security and Risk Management (FIPS Pub 31)
- Computer Security Guidelines for Implementing the Privacy Act of 1974 (FIPS Pub 41) – Withdrawn November 18, 1998 because it is now considered an industry standard – No replacement publication will be issued.
- Guidelines for Security of Computer Applications (FIPS Pub 73)
- DoD Rainbow Series Library at http://www.radium.ncsc.mil/tpep/library/rainbow/index.html.

Requirements

The following table includes the TIERS security requirements that must be complied with by TDHS and vendor staff. It should be noted that the requirements provided in the table are still in the process of being reviewed by the TDHS Security Workgroup.

TIERS SECURITY REQUIREMENTS
Login Requirements
All log-on security must be at the individual level, not global.
The system must automatically log out after specified inactive time.
The system must not allow more than one log-on per person unless authorized by the State.
The system must suspend a log-on ID after three access attempt failures.
The security administrator must assign a log-on ID that is different than a person's Social Security Number (SSN). It is a privacy issue to use SSN as a user ID.
The security administrator must provide user log-on security clearance including a separate log-on identifier for each authorized user.
The log-on ID must permit access to the system only in combination with a valid password.
The security system must provide the ability to automatically restrict an individual to one log-in location at a time.
The application must provide Userid tracking through all levels of the system.
Log-on ID and passwords must be controlled through both a central agent, serving as a security officer for the application, and a local office security officer which could be a non-technical user.
Password Requirements
The system must prohibit access by unauthorized users to the security sub-system.
The system must encrypt passwords moving throughout the network, with special consideration given for dial-in access.
The system must prohibit password reuse and maintain password history of previously used passwords for 10 intervals.
The system must provide automatic password expiration and change

enforcement.
The security sub-system must allow for multiple levels of security and support local security administration, as well as centralized security administration.
Security must reside with the application to limit the menus, screens and functions (e.g., update) that a user is authorized to access.
The levels of application system security must be changeable only by the appropriate management staff to change security levels without the assistance of technical specialists, such as programmers.
Audit and Reporting Requirements
The system must provide the ability to track activity logging and reporting including table updates by individual identifier.
The system must provide on-demand audit reporting of activity including a daily audit log of update transactions.
The system must provide the ability to generate reports from logged data.
The system must provide Auditors the ability to determine the modifications applied to a record over time and identify the users who changed the data.
The system must provide an audit trail of all access, including updates to the database and system tables. At a minimum, the system must provide a log of the audit trail which includes: • User ID • Time of Activity • Type of Activity • An indication of each transaction's success or failure • An identification of the record accessed • Any changed data • Device Used.
Field and Data Requirements
Field level security must be included in the system to prevent users with

access to a specific record from modifying certain sensitive data within that record.
Once a user has accessed the system, controls must be implemented to limit that access to only the specific data for which the user is authorized.
The system must provide an on-line means to assign, update or remove on-line access and authorization for individual users.
Data must be secured system against unauthorized access at the application program, system software, data item, record, database and transaction level.
The system must provide access to Ad Hoc report generation programs must be limited to authorized users.
Other Miscellaneous Requirements
Security administration will be performed by TDHS.
The system must provide a method to access both legacy and TIERS applications to support a seamless transition.
The system for the TIERS application should be designed as a separate application layer to minimize the impact on the overall application.
The TIERS application will follow the current security administration model.
Define application security through the use of standard profiles.
The security process must be table-driven to permit an authorized non-technical user to manage security and serve as the security administrator.

Maintain Profiles

Profile tables must contain all required data to support the various processes of the system. These profiles must enable TIERS to control access to data. TIERS must have the ability to print out any of the profile tables in summarized form.

Maintain User Profile

User profiles must include, but are not limited to, the following data elements:

- User name and ID

- Telephone number and FAX number of a user
- Office location
- Supervisory unit assignment
- Work hours
- Security access authorization

Maintain Office Profile

A Region will have more than one location. Each Office location must have a profile table that includes, but is not limited to, the following data elements:

- Name of the office
- Location of the office
- Office hours
- Geographic boundaries
- Program types that are handled at that location
- Off-assignment indicator that indicates if the location can receive case transfers

Provide Authorized Access

Provide Authorized Access to the Application

- TIERS must ensure that only authorized users have access to the system and can perform only those functions for which they are individually authorized.
- User log-on and password security clearance must include separate log-on identifiers for each authorized user. The log-on ID must permit access to TIERS only in combination with a valid password. Log-on IDs must be controlled through an authorized user, serving as a security administrator for the application. Initial clearance into TIERS must be through the Security process.
- TIERS must include a transparent connection to the host and server that only requires a single sign-on by the user. There will be a single security system for all TDHS applications and passwords must be changed periodically.

- All user log-ons must require a password validation. Each user must be capable of changing their password at their discretion. Passwords can only be changed by the user.

- Password characteristics must be defined by State criteria.

- Passwords and defaults must be encrypted into the system.

- A security administrator must have the ability to reset passwords to a default password. Default passwords must be changed before access is allowed to perform case activity by the user.

- Dial up access to TIERS from external users (outside sources) requires that the implementation of security access be consistent with measures to meet existing standards. Usage for external users must be limited based upon the rules, regulations, policies, and procedures governing such access of TIERS data.

Provide Authorized Access To Data

- Authorized access to TIERS data must be restricted through a combination of user level security based upon the User Profile. In addition, there is a need for security controlled access to certain data elements within non-confidential cases.

- User profiles must be defined based on job function. The security administrator must be able to modify access to TIERS for individual users, as appropriate. For example new users or users on probation may need to have limited access to authorize case transactions. TIERS must allow for supervisory review/approval of specified transactions by users.

- Field level and transaction level security must be included in TIERS to prevent users with access to a specific case record from viewing or modifying certain sensitive data within the record. The physical location ofTDHS client sensitive data is protected.

- Any change to data must be saved and updates stored for a specified time period. This provides ability to recreate previous data if necessary.

- Auditors must be able to determine the modifications applied to a case record over time and identify the users who made the changes. Each transaction must be logged and contain at a minimum user identifier, workstation identifier, and case specific information. The transactions logged must be maintained for ad hoc reporting.

- TIERS must provide the ability to designate a specific percentage up to 100% monitoring and logging of transaction activity for designated users.

Security for System Test , User Test and Training

The test and training functions must be kept either physically or logically separate from production functions. Copies of production data must not be used for testing or training unless the data has been declassified or unless all personnel involved in testing and training is otherwise authorized access to the data. Appropriate information security and audit controls must be incorporated into new systems. Each phase of systems acquisition must incorporate corresponding development or assurances of security and auditability controls.

Audit trails must be provided that meet professional electronic data processing audit and control standards as set by the American Institute of Certified Public Accountants and the United States General Accounting Office. Audit trails must be able to trace the manipulation of any data within the database to a time and user identifier, and must provide for recovery of any update transaction in process during a hardware or software failure.

Disaster Recovery Plan

Standards

The vendor must develop a Disaster Recovery Plan detailing the methodology for the recovery of hardware and software functionality based on the requirements identified below. The vendor will utilize existing State recovery sites/infrastructures which are in place today, including, but not limited to the West Texas Disaster Recovery and Operations Center, to the extent that it can be integrated into the vendor's overall solution.

Requirements

Procedures and facilities are required to be in place to ensure Disaster Recovery within a twenty-four (24) hour/day period. *In the event of major problems at the Data Center, or any State office, the vendor must provide an alternate means of assuring system availability.* This includes, but is not limited to, hardware, software, and communications. The requirements for disaster recovery are identified below:

- The system must have the ability to restart communications and associated applications following a non-disaster system failure. This restart ability must:

  ⇒ Restore all system files to their State of completion as of the last fully processed transaction
  ⇒ Provide a notification ability, at the operator's discretion, to broadcast to all active devices that the system is once again operational and

⇒ Provide for this notification to be automatically and manually initiated

- Restoration of databases must automatically process all transactions completed prior to the loss of the system. Once the system becomes available again, it should only be necessary for system users to re-enter the transactions that were in progress at the time availability was lost.

- The system must provide for all databases to be completely restored as they were before the loss of the system.

- The back-up/restore process for the enterprise databases must be simple, economical, certain, and must not adversely impact the system availability requirements. It is anticipated that the back-up/restore process for any locally stored data would take substantially less time than the enterprise server database.

- Back-up and restoration of local databases residing on local servers must not require operator intervention at the local site with the exception of inserting a tape or other storage medium (e.g., CD-ROM).

- Backup and recovery solutions must include back-up and recovery processes for both data and software. All TIERS databases must be demonstrated to be fully recoverable within time frames consistent with the business requirements for TIERS.

- Backup and recovery solutions must support full and incremental backups to reduce time spent performing backup functions.

- Backup and recovery solutions must provide security against unauthorized access.

- Backup and recovery solutions must support backup to multiple media types (e.g. tape, disk, etc.).

- Backup and recovery solutions must support attended and unattended backup.

- Backup and recovery solutions must provide the ability to list the contents of a backup without performing a recovery.

G. Performance Specifications

Overview

Performance Standards

The vendor is responsible for meeting negotiated standards for the measurable performance of specified system components. *The vendor must monitor these components and report their levels of performance to TDHS.* The primary areas of measurable performance are:

- service request response times
- operational throughput
- system availability

Business Needs Drive Performance Standards

Staff productivity and customer satisfaction will be weighed against the cost of performance when negotiating performance standards. All performance standards must be consistent with, and supportive of, all applicable governmental legislation, regulation, and litigation.

Technical Design

The vendor must develop a technical solution within the TDHS constraints identified which appropriately distributes the workload of the system across all components, whether managed by the vendor or some other entity. The technical system design developed by the vendor will be evaluated from total cost and total performance perspectives to insure that it does not unduly shift work from components under its management to components it does not manage.

Monitoring

Because the system will be utilizing IT resources not managed by the vendor, performance monitoring must be discrete enough to attribute all portions of the performance measure to the appropriate responsible party. *The vendor will be responsible for that portion of the performance measure attributable to resources managed by the vendor. The vendor will be responsible for providing expected levels of performance and anticipated workloads for resources not managed by the vendor to those entities responsible for their management. The vendor will also be responsible for identifying and reporting on shortages in resources provided by those entities that prevent acceptable levels of total system performance to TDHS.* An example is provided in Figure 7.

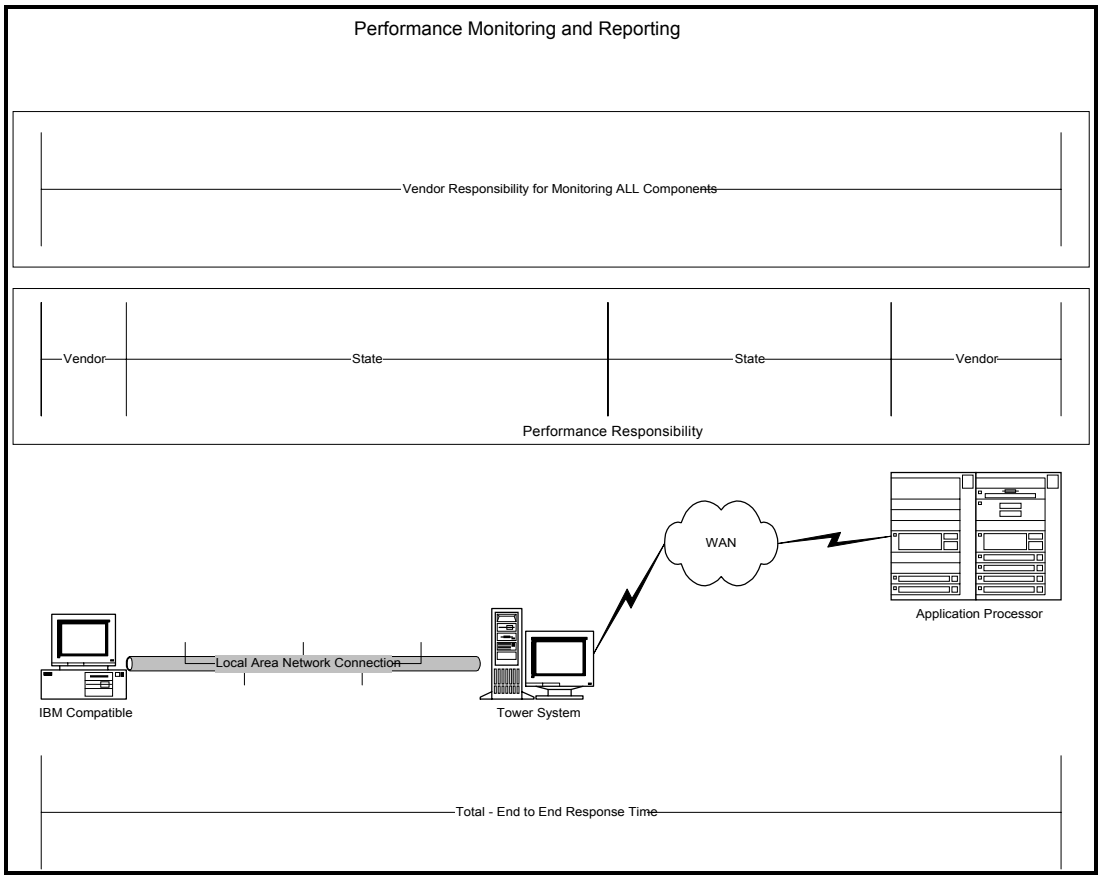


Figure 7 - Performance Monitoring and Reporting Example

Service Request Response Times

Response Time Defined

Service request response time is defined as the time interval between the submission of the request for service by a user of the system or another component of the system and the completion of delivery of the service or request outcome to the requester.

For an interactive service request, the response time is the interval from the point at which the workstation operator depresses the last appropriate key in the initiating sequence to the point at which the complete and total response, with appropriate information, appears on the screen and the workstation is available to respond to operator input.

For a print initiation service request, the response time is the interval from the point of completion of the print request to the completion of the placement of the document in the print queue.

Performance standards governing service request response times will be established on a service by service basis driven by the business needs to fully utilize staff time and to provide quality service to the client.

Interactive Service Request

The most demanding performance standards will be assigned to those services supporting business activities involving the direct interaction of staff with clients. These activities are heavily dependent on a highly interactive GUI with the system. There are two ways in which interactive service requests will be processed:

- real-time service – requester waits for service delivery to continue process
- queued – requester continues processing while service is being delivered.

Whether a given service is to be provided in real-time or is to be queued is determined by the business needs associated with that service as weighed against the relatively higher cost of real-time delivery compared to queued delivery.

Response time requirements will be of the form: "N percent of all occurrences of this service request must be honored within time interval M^1 and all occurrences within interval M^2."

All telecommunication time is included in the response time measurement. It is the responsibility of the vendor to determine if existing networks, if included in the solution, provide enough bandwidth to meet the requirements. *The vendor must also supply an enhancement plan if the current network configuration is in need of expansion.*

Operational Throughput

Batch Processing

TIERS batch processing must be completed within the time frames determined by TDHS.

The IT components of the TIERS system must have the capacity to not only meet the demands of interactive service requests within negotiated performance standards during peak periods, but also to meet the batch processing requirements during off-peak periods. IT components involved in batch processing must have enough capacity to permit all on-line functions to execute against accurate, up-to-date data during standard operational hours while accumulating no backlog in batch processing within a period greater than 24 hours.

System Availability

TIERS System on-line functions executed on the desktop, laptop, and from other devices, as needed, must be available during standard operating hours. TIERS must be available for on-line and batch functions ninety-nine point five percent (99.5%) of the time. This requirement should be interpreted to include all aspects of the system including, but not limited to, workstations, local/regional servers, enterprise servers, communications channels, printers, etc.

APPENDIX A

TIERS Product Standards

Component	Product(s)
Servers	RISC = HP or SUN Enterprise or SUN Workgroup line Intel-based = any Microsoft certified platform
Server OS	UNIX (HP-UX or Solaris), NT or Novell
Desktop	on TDHS contract
Desktop OS	Windows 2000
Laptop	on DIR contract
Laptop OS	Windows 2000
Desktop OS additions	MS Internet Explorer MS WORD MS Exchange/Outlook Symantec Virus Detection

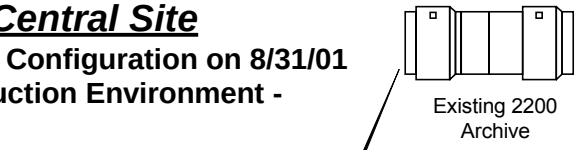
APPENDIX B

NOTE: The following diagrams apply to the anticipated TIERS Technical Architecture for the 8/31/2001 pilot.

last update:5/8/00 2:02 pm

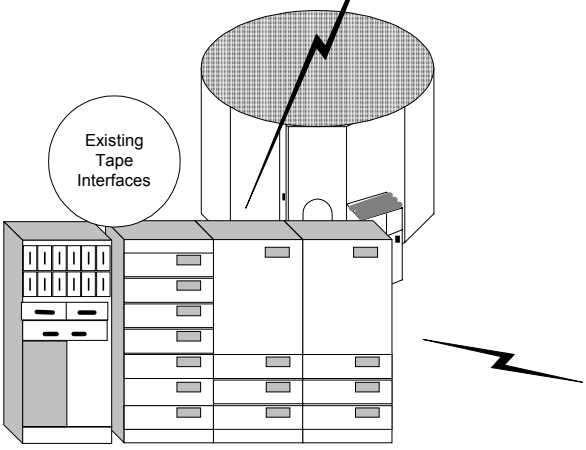
Central Site

TIERS Pilot Configuration on 8/31/01
- Production Environment -

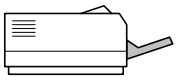


Functionality of 2200:
- Very large % of existing SAVERR including benefit authorization, reporting
- Current systems outside SAVERR
- Continue existing data exchanges outside of Pilot
- Communicate with WebSphere
- Run/monitor transactions across multiple platforms
- Access to mass storage devices (tape silos)

Software on 2200:
OS2200
RDBMS (ANSI92)
DMS -1100
TIP
COBOL
3270 emulator (COM SW: BSC 3270R on both DCPs)

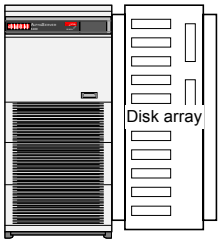


UNISYS 2200 (1)

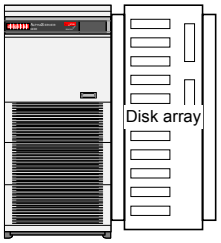


Existing High
Speed Printer(s)

NOTE: The UNISYS 2200 is headed toward retirement. Our expectations are for all work done on the 2200 to migrate to other more Open platforms before 2007.



ORACLE RDBMS
Server (1)



ORACLE RDBMS
Reporting
Database Server (1)

Functionality of RDBMS platform(s):
- Store data from all case actions in the pilot
- Communicate with Transaction Servers
- Run Stored Procedures (SPs to be minimized, but used for higher performance)
- Store archived data from the pilot
- ECF storage & retrieval

Software on RDBMS platform:
UNIX (Solaris)
ORACLE DB - current version at time of development
VERITAS
BMC Patrol

Functionality of Reporting platform:
- Provide data manipulation to create reports
- Provide data for reports

Software on RDBMS Reporting platform:
UNIX (Solaris)
ORACLE DB software - current version
Perl
Report Formatting software
BMC Patrol
VERITAS

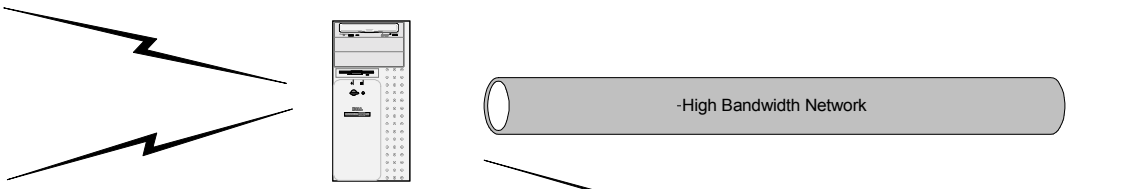
NOTE: Central Site will also include Nodal and Local Office Configurations

last update:5/8/00 2:02 pm

Central Site

TIERS Pilot Configuration on 8/31/01
- Production Environment -

Functionality of Transaction Server: • Connection pooling to all data and application servers • Provide 'single points' of security • Event management & registration • Fault management, routing, load balancing • UNISYS connectivity	**Functionality of INTRAnet Information Server:** • Pass data and application request through to Application Server • Format and ship pages to client
Software on Transaction Server: UNIX (HP-UX or Solaris) IBM WebSphere	**Software on INTRAnet Server:** UNIX (HP-UX or Solaris) WebSphere Internet Server - version current at time of deployment



Application, INTRAnet & Transaction Server (1)

Functionality of Application Server: • Execute application code modules • Communicate with the Database Servers (and later separate Application Servers) to get needed data & executables
Software on Application Server: UNIX (HP-UX or Solaris) IBM WebSphere Coding languages (as determined by Application Server product: expected to be primarily JAVA based using EJBs)

DELL 6300
Central Asset Management Server (3)

Connects to Nodal Asset Mgt. Servers

Functionality of Asset Mgt. Server • Asset Management support including Software Distribution • May or may not be able to combine this on another platform • One used as Central Server, two others as staging SMS servers
Software on Server SMS 2.x

Connects to Nodal Directory Services

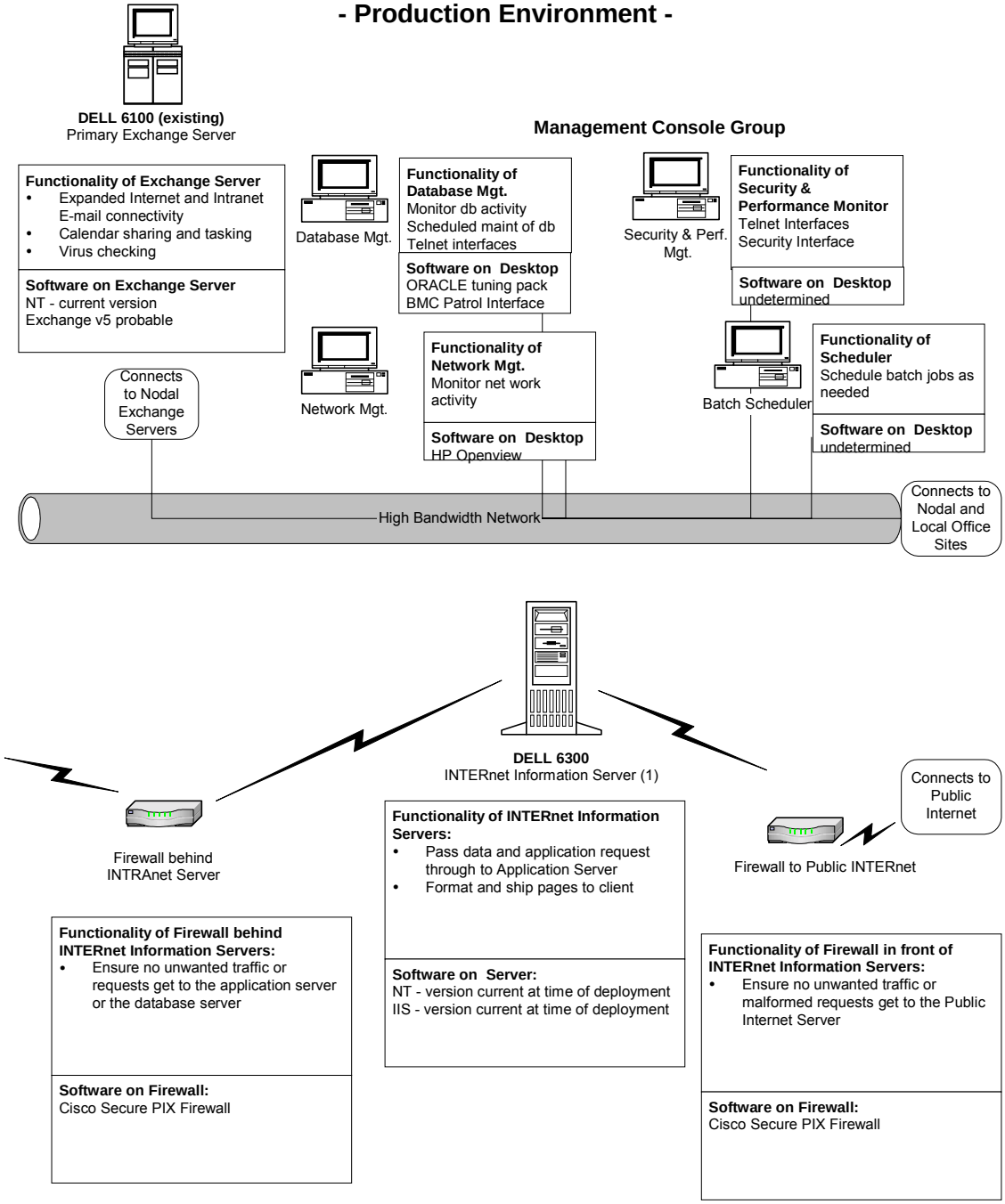
DELL 6300
Directory Services Replication Server (1)
a.k.a DS Replica Server

Functionality of Novell Directory Server Novell Directory Server
Software on Server NDS v8.x

NOTE: Central Site will also include Nodal and Local Office Configurations

Central Site

TIERS Pilot Configuration on 8/31/01
- Production Environment -

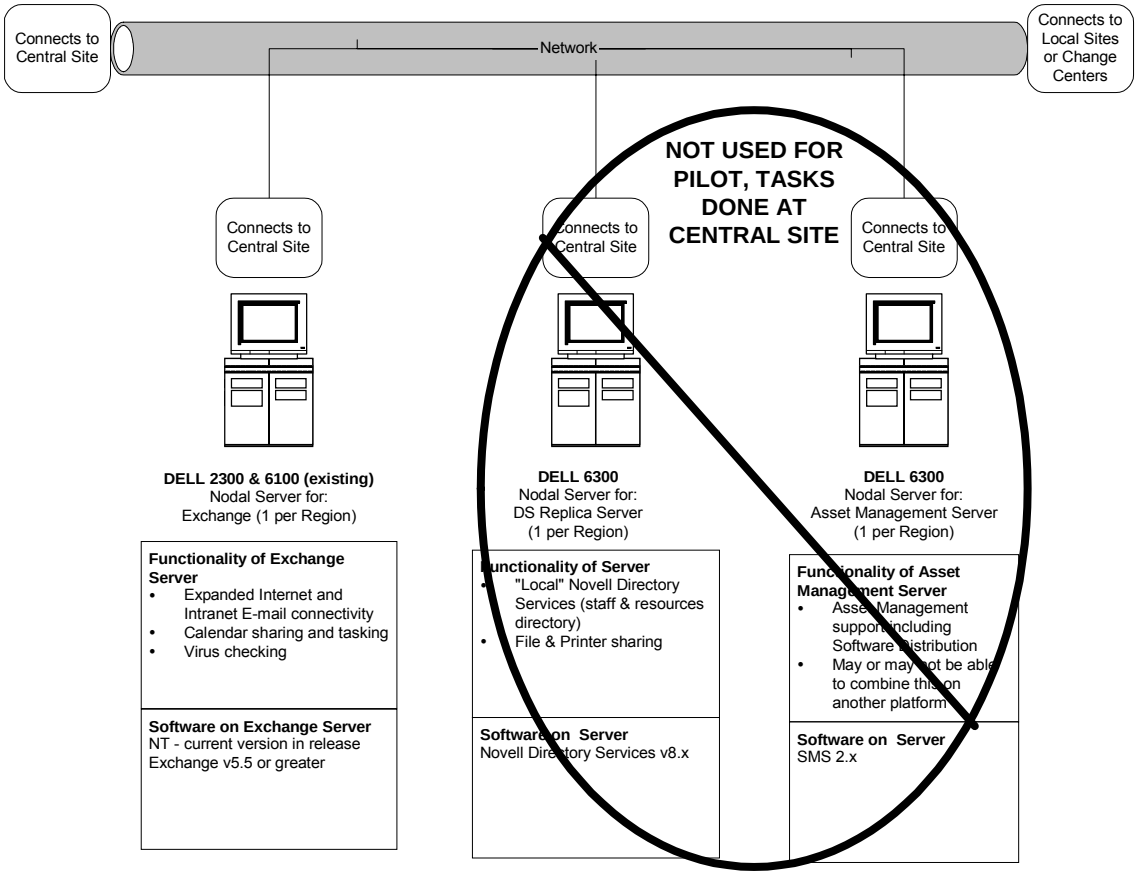


NOTE: Central Site will also include Nodal and Local Office Configurations

last update:5/8/00 2:02 pm

Nodal Site

TIERS Pilot Configuration on 8/31/01
- Production Environment -

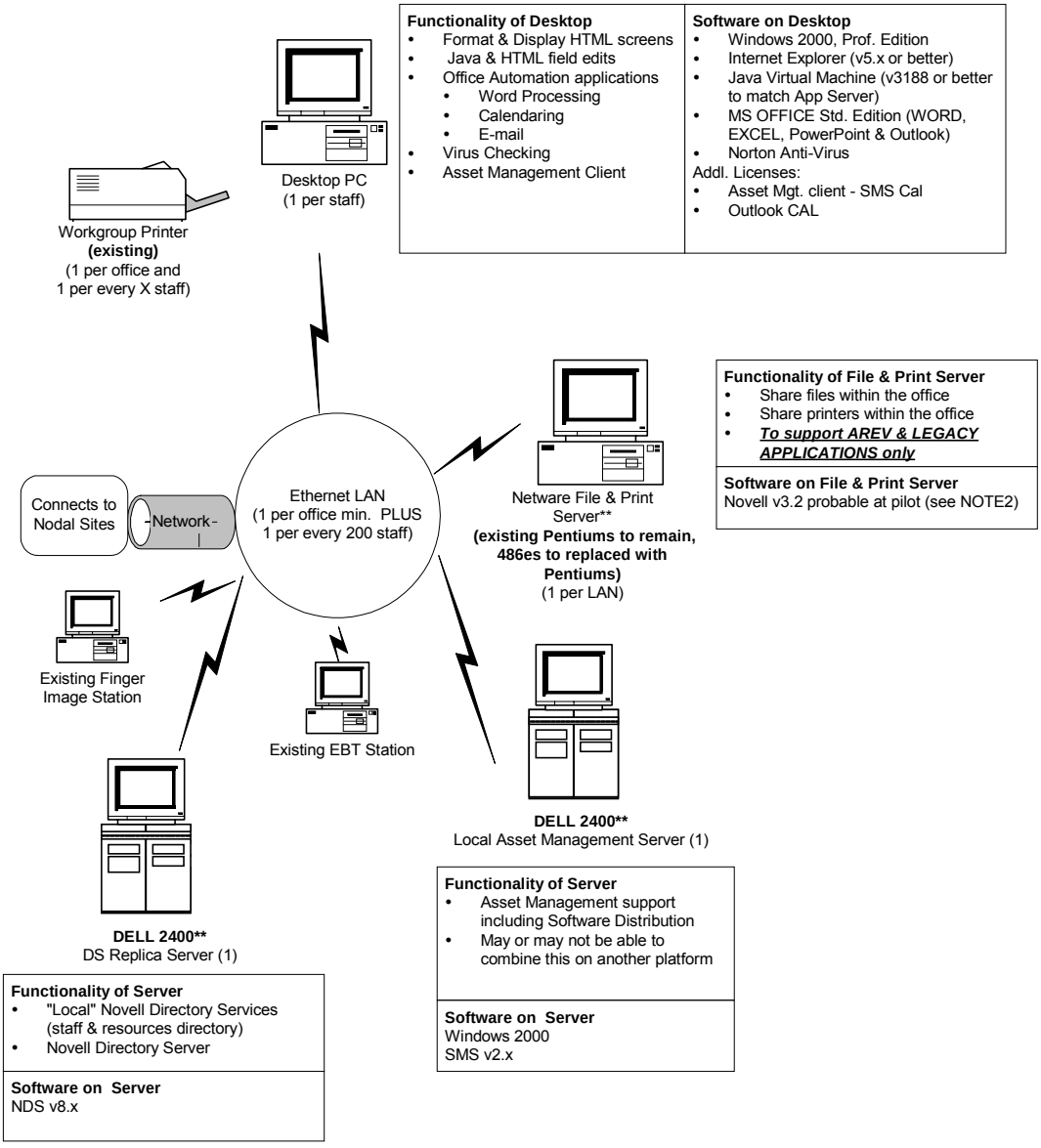


NOTE: Each Nodal Site has a Primary Domain Controller, a Secondary Domain Controller and a Backup Domain Controller. Domain Controllers provide DNS services and 5 of them may be useable for the Nodal Asset Management servers. The rest are currently workstation caliber platforms, not servers.

NOTE: Nodal Sites will also include Local Office Configurations

Local Office Site

TIERS Pilot Configuration on 8/31/01
- Production Environment -



**** NOTE1:** The DS Replica Server, the Local Asset Management Server and the Netware File and Print Sever will only be installed in those offices that have over 10 staff. For smaller offices, these services will be provided by the platform at the Nodal Sites. All of the planned Pilot offices are expected to have a minimum of 30 staff.

NOTE2: After the pilot, the Netware File & Print Server platform will assume the tasks of both the DS Replica server and the Asset Management Server. This is dependent on hardware and software upgrades.